



US010924575B2

(12) **United States Patent**
Åström et al.

(10) **Patent No.:** **US 10,924,575 B2**
(45) **Date of Patent:** **Feb. 16, 2021**

(54) **AUTOMATIC NETWORK MANAGEMENT SYSTEM AND METHODS**

(71) Applicant: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(72) Inventors: **Bo Åström**, Stockholm (SE); **Stephen Terrill**, Villanueva de la Cañada (ES)

(73) Assignee: **Telefonaktiebolaget LM Ericsson (publ)**, Stockholm (SE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 98 days.

(21) Appl. No.: **16/313,773**

(22) PCT Filed: **Jul. 18, 2016**

(86) PCT No.: **PCT/SE2016/050724**

§ 371 (c)(1),
(2) Date: **Dec. 27, 2018**

(87) PCT Pub. No.: **WO2018/004413**
PCT Pub. Date: **Jan. 4, 2018**

(65) **Prior Publication Data**
US 2019/0158617 A1 May 23, 2019

(30) **Foreign Application Priority Data**
Jun. 29, 2016 (WO) PCT/SE2016/050659

(51) **Int. Cl.**
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC **H04L 67/2823** (2013.01); **H04L 63/102** (2013.01); **H04L 63/20** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC H04L 67/28; H04L 67/2823; H04L 63/20; H04L 63/102; H04L 63/205; H04W 72/04; H04W 76/10; H04W 72/048; H04W 76/15

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,135,809 B2 3/2012 Hehmeyer et al.
2010/0309872 A1* 12/2010 Amini H04W 74/002 370/329

(Continued)

FOREIGN PATENT DOCUMENTS

CN 101989923 A 3/2011
CN 104468162 A 3/2015

(Continued)

OTHER PUBLICATIONS

International Search Report and Written Opinion issued in International Application No. PCT/SE2016/050724, dated Feb. 24, 2017, 10 pages.

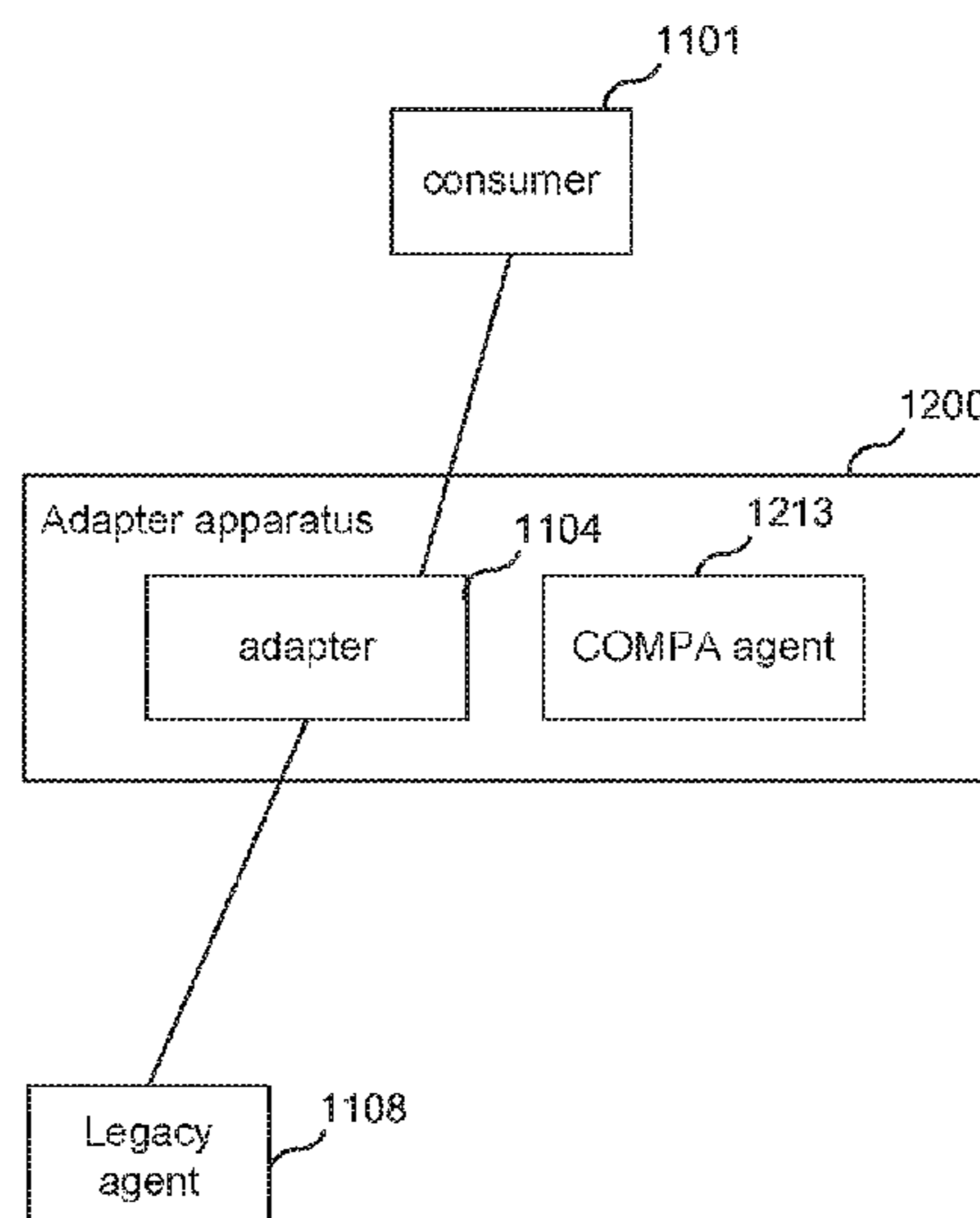
(Continued)

Primary Examiner — Rownak Islam
(74) *Attorney, Agent, or Firm* — Sage Patent Group

(57) **ABSTRACT**

A network management architecture referred to as the Control/Orchestration/Management/Policy/Analytics, COMPA, architecture. The COMPA architecture functions to simplify and automate the operations (both management and business process) of a network. In one aspect, the COMPA architecture provides controlled access to functionality provided by different responsibility domains using cooperating service access control, SAC, agents.

18 Claims, 23 Drawing Sheets



- (51) **Int. Cl.**
H04W 76/15 (2018.01)
H04W 72/04 (2009.01)
- (52) **U.S. Cl.**
CPC *H04L 63/205* (2013.01); *H04W 72/048*
(2013.01); *H04W 76/15* (2018.02); *H04L*
67/28 (2013.01)
- (58) **Field of Classification Search**
USPC 370/329
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0289027 A1 11/2011 Moore
2014/0281292 A1 9/2014 Isaacson et al.
2015/0349934 A1* 12/2015 Pollack H04L 5/0055
370/329

FOREIGN PATENT DOCUMENTS

CN 105207882 A 12/2015
WO 2008068233 A1 6/2008

OTHER PUBLICATIONS

First Office Action dated Dec. 28, 2020 for Chinese Patent Appli-
cation No. 201680087043.5, 20 pages.

* cited by examiner

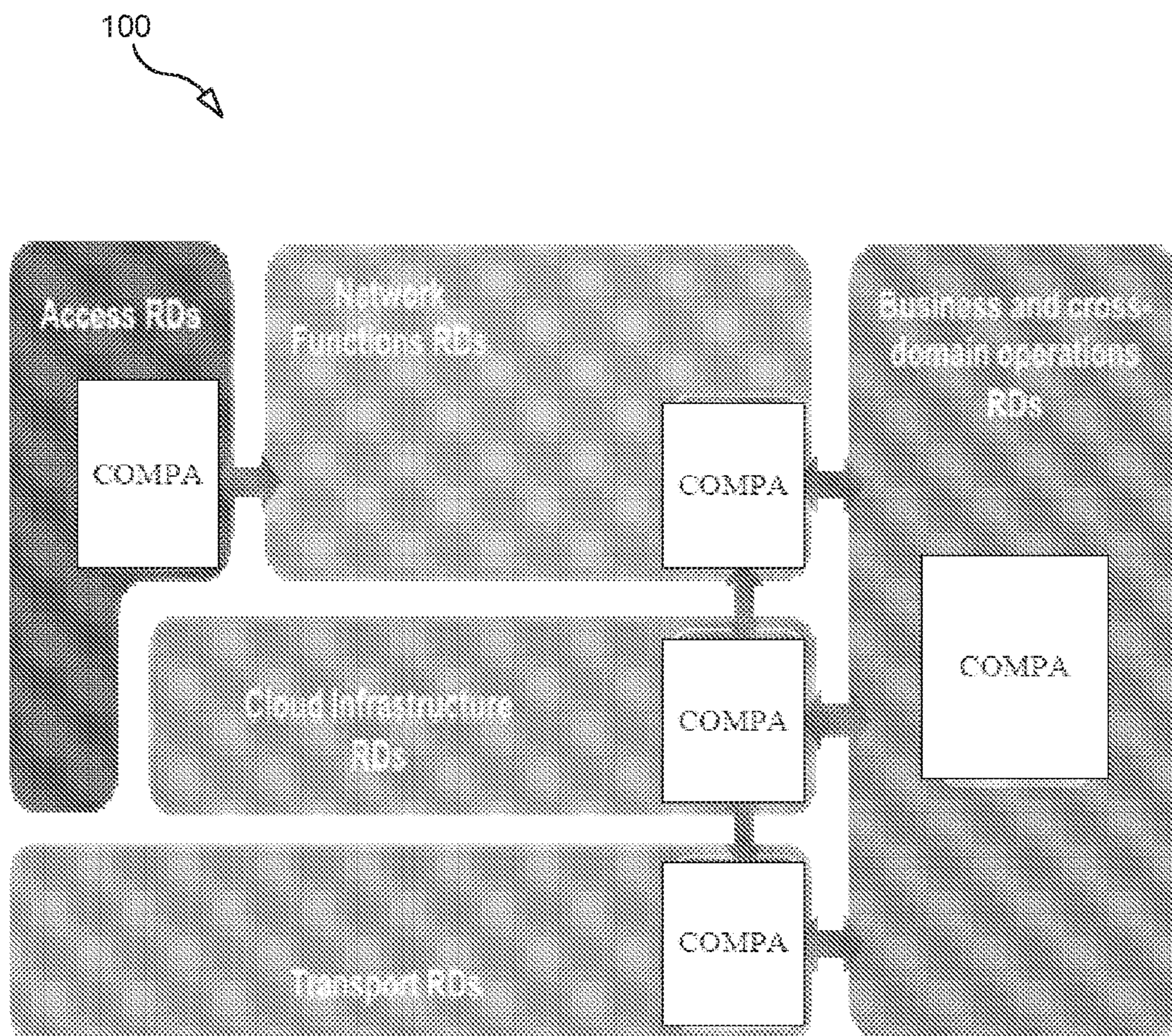


FIG. 1

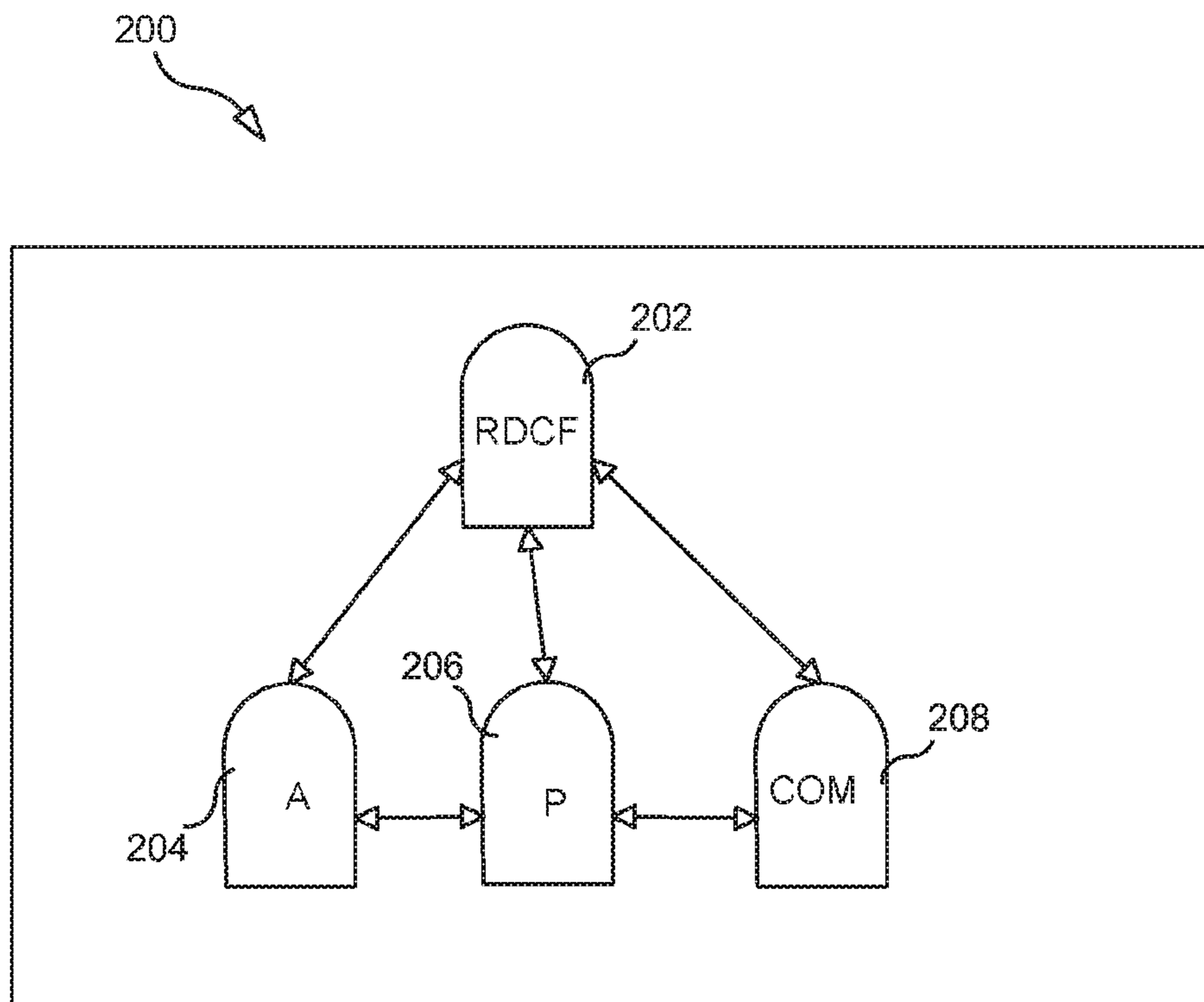


FIG. 2

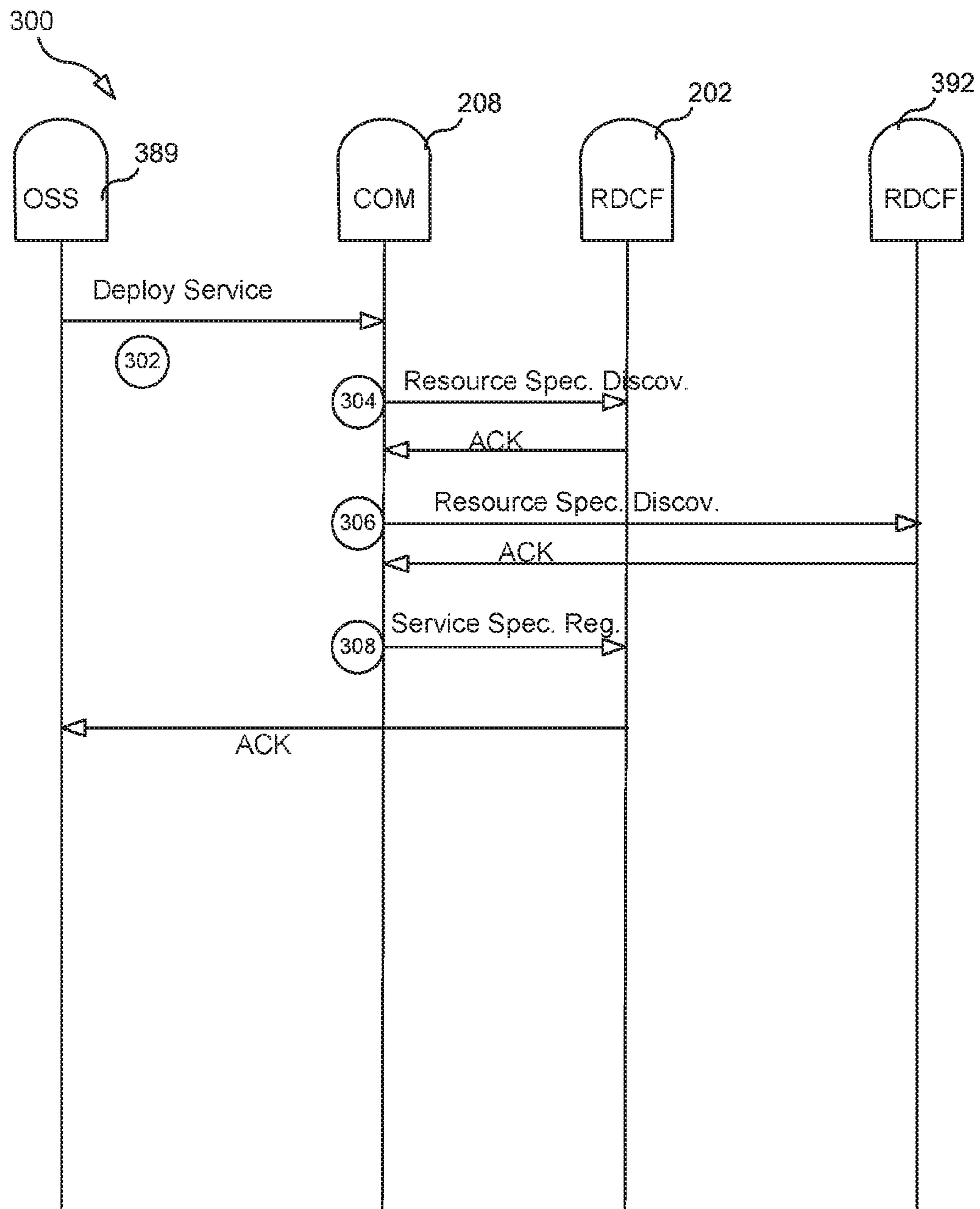


FIG. 3

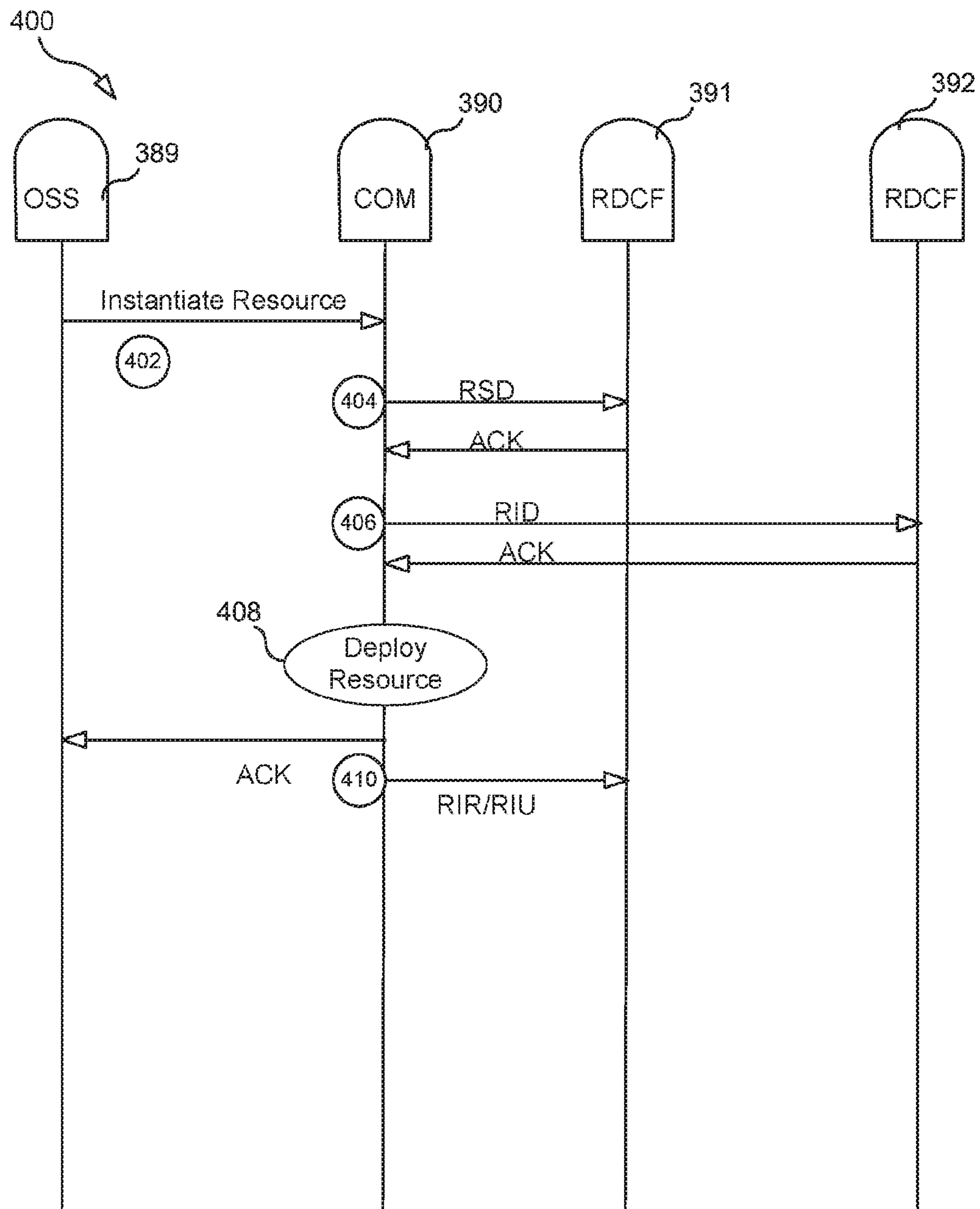


FIG. 4

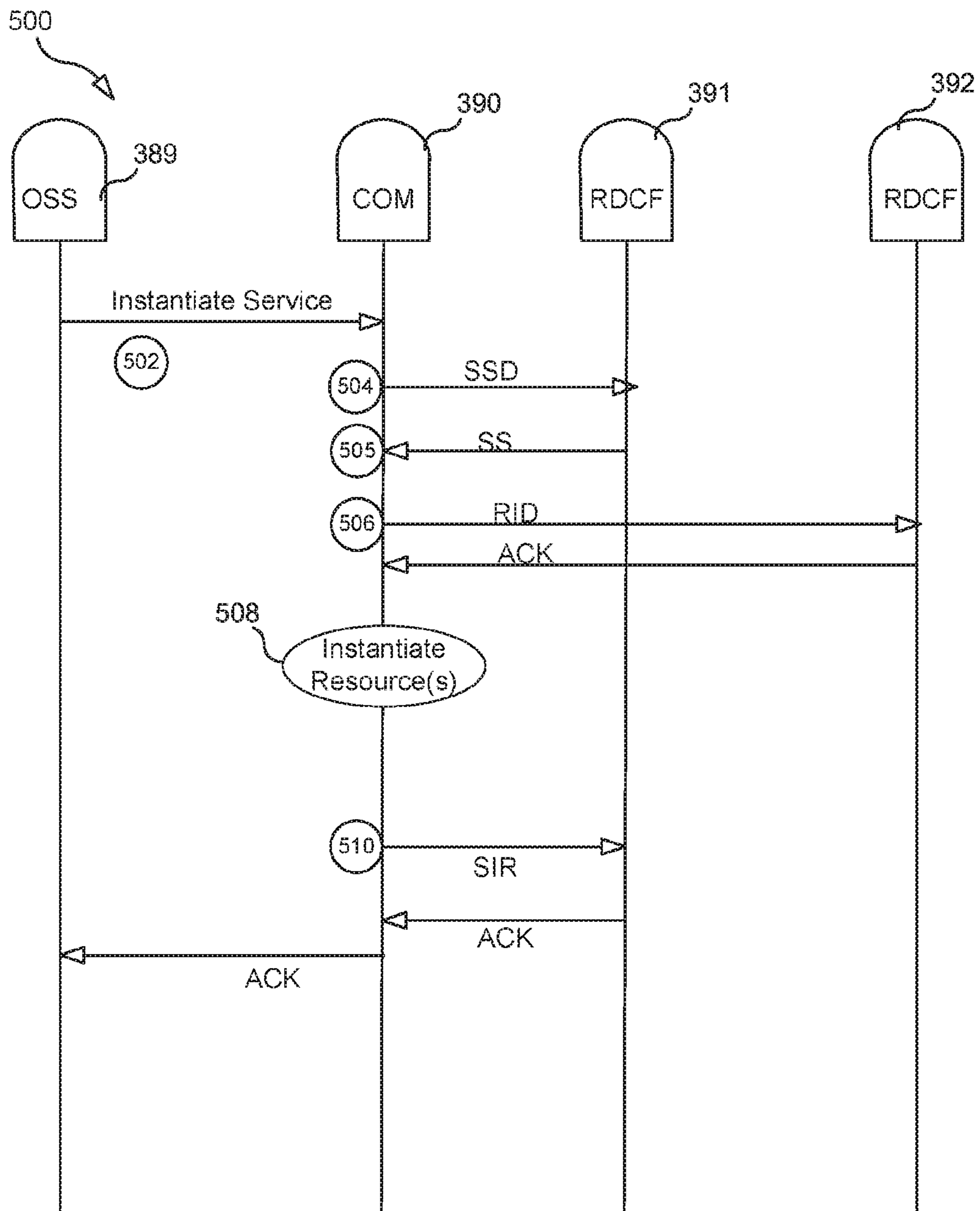


FIG. 5

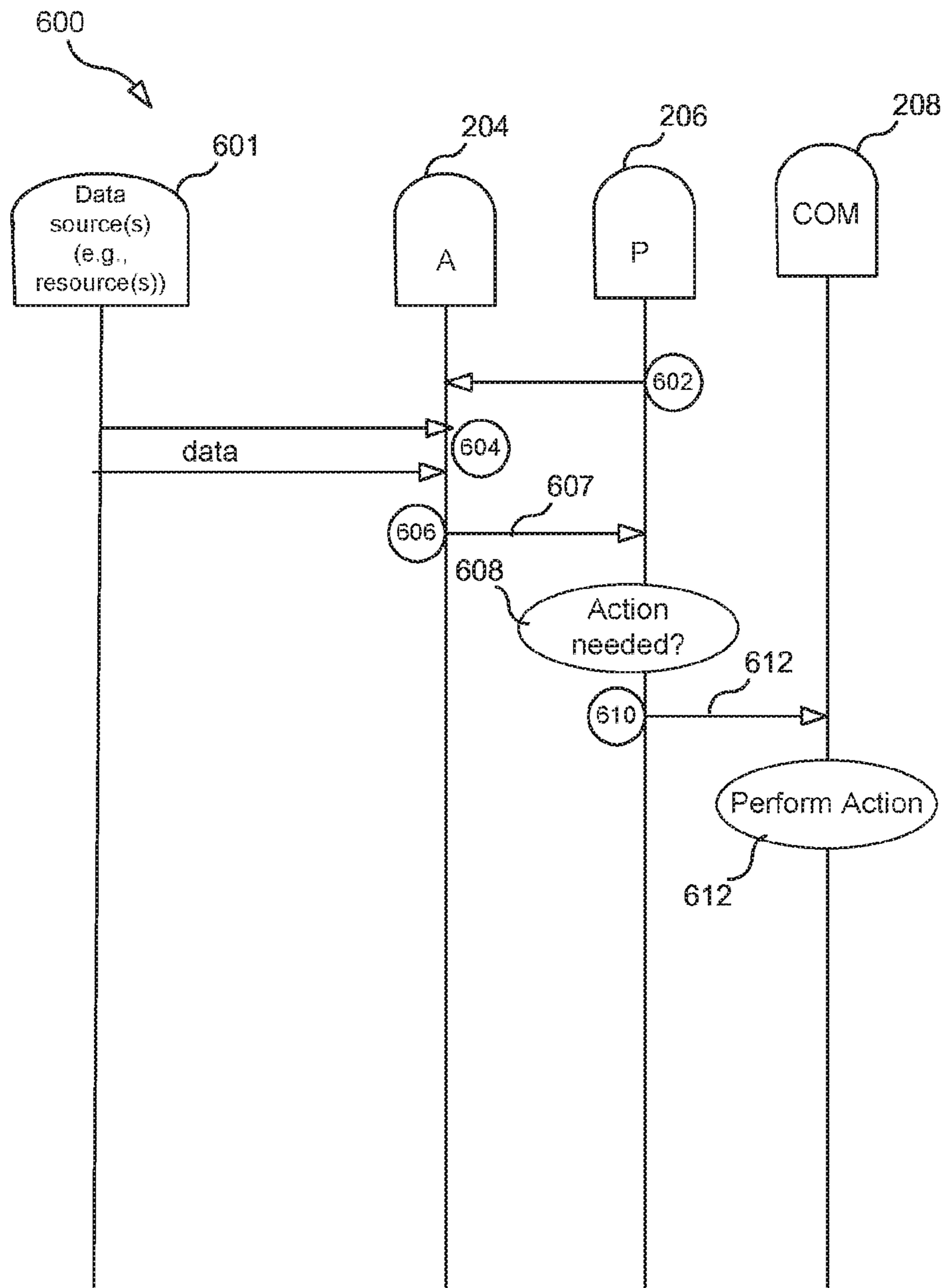


FIG. 6

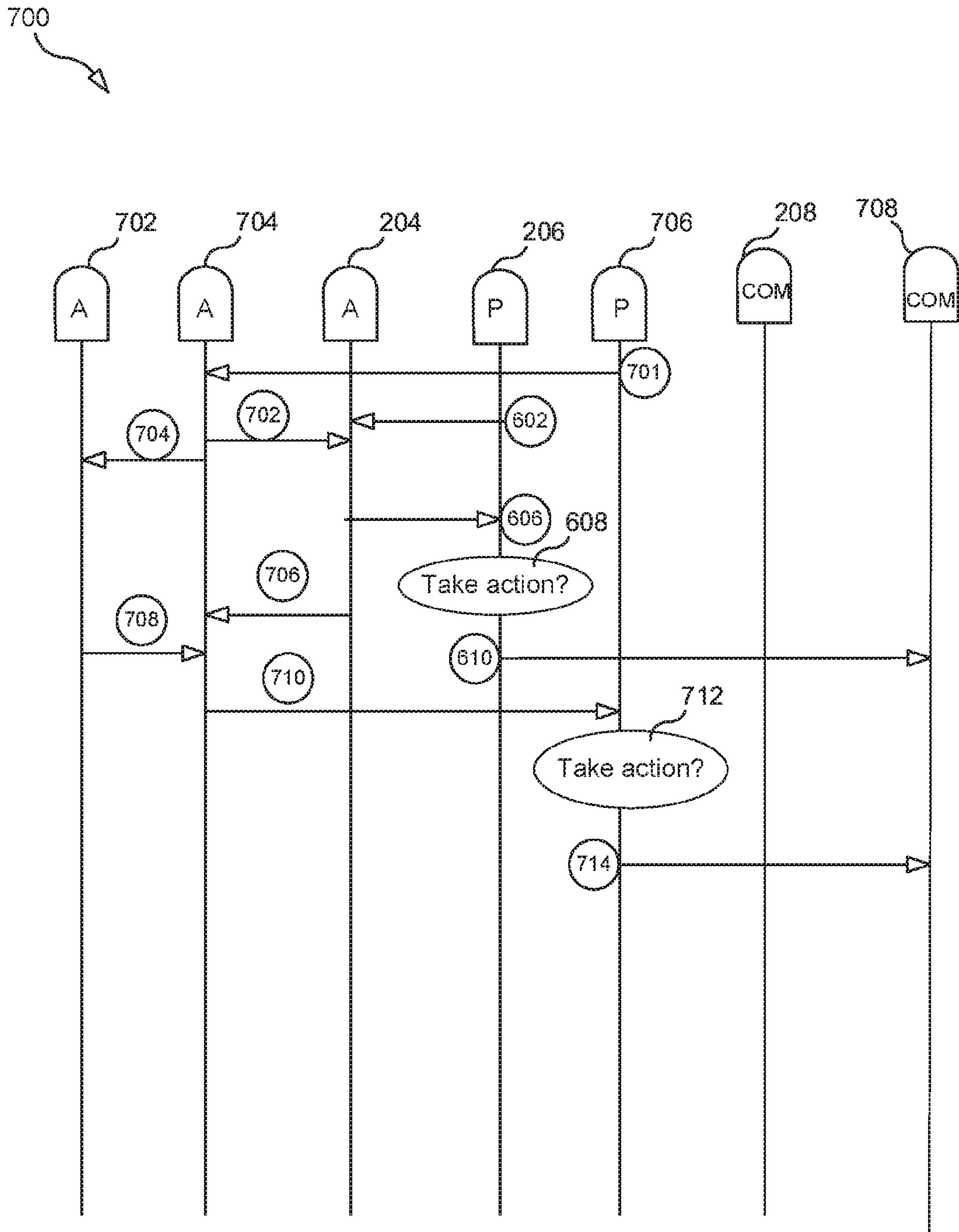


FIG. 7

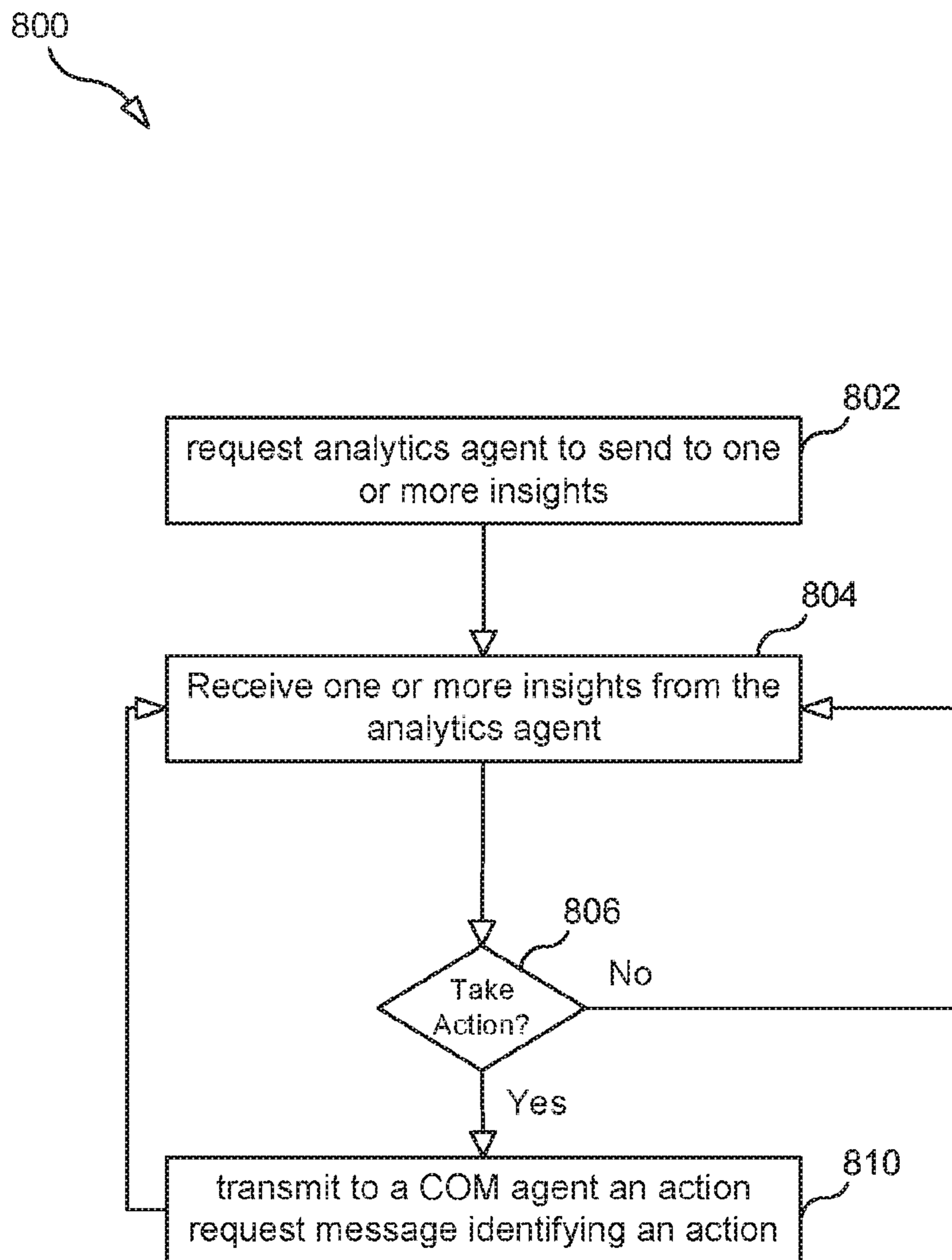


FIG. 8

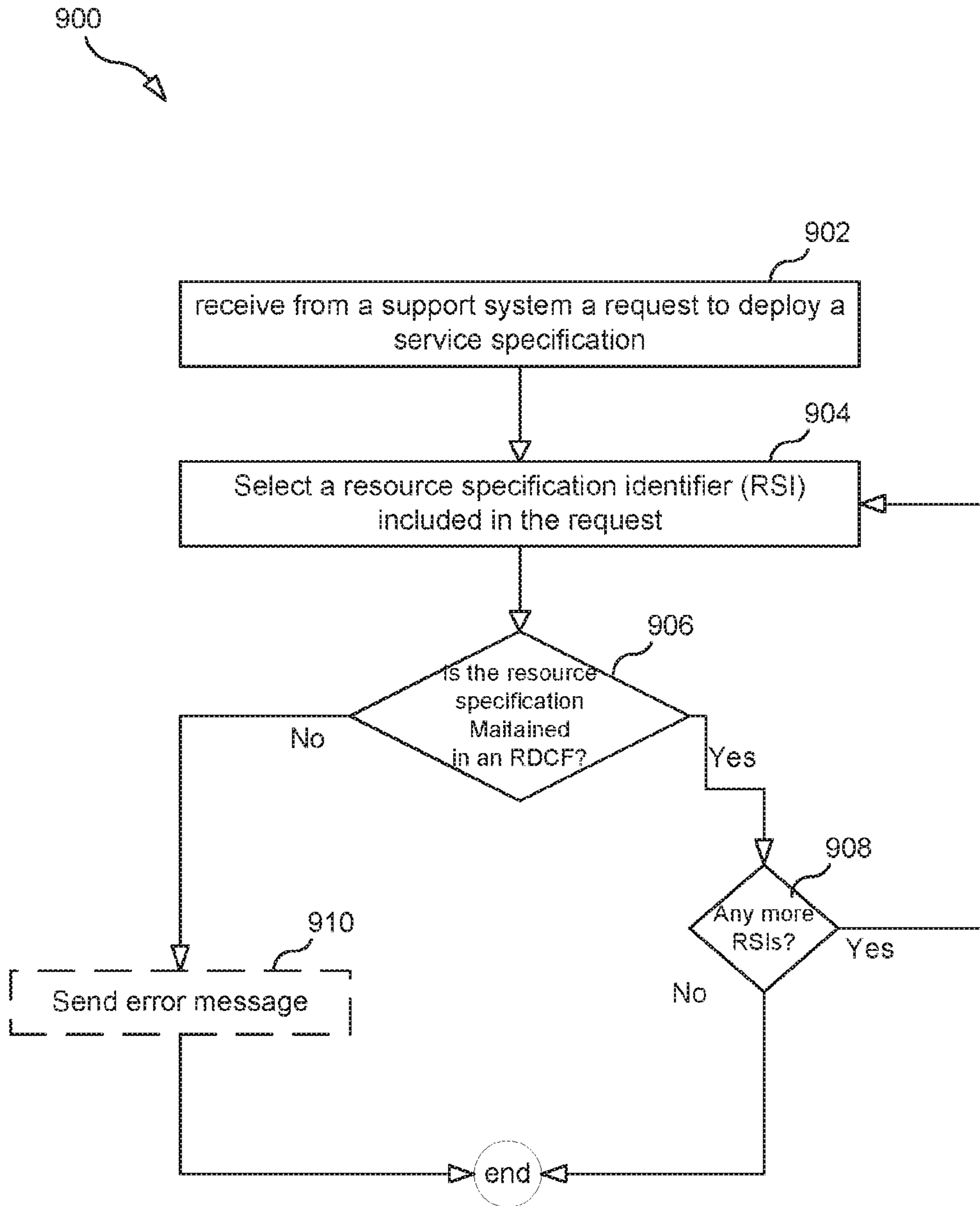


FIG. 9

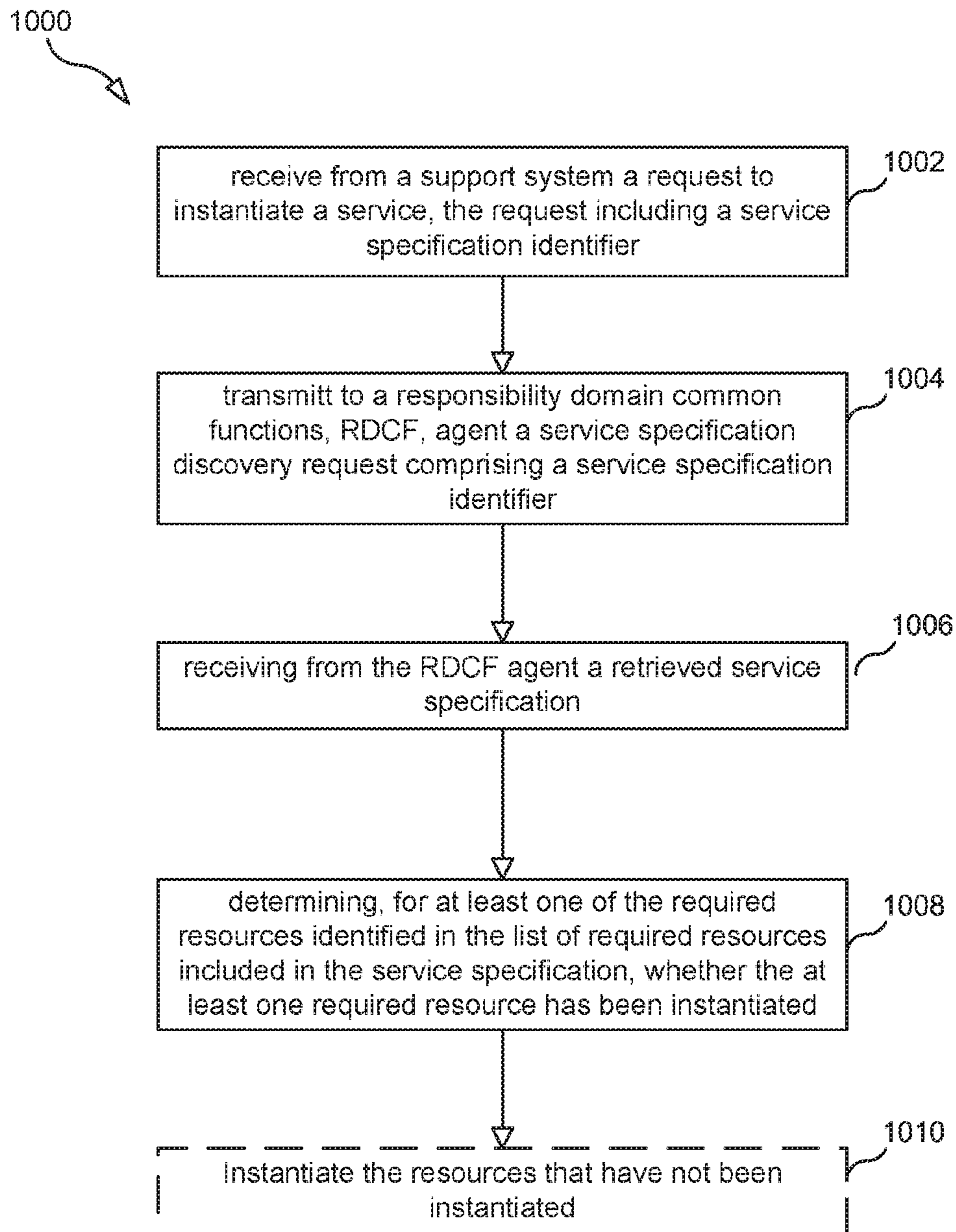


FIG. 10

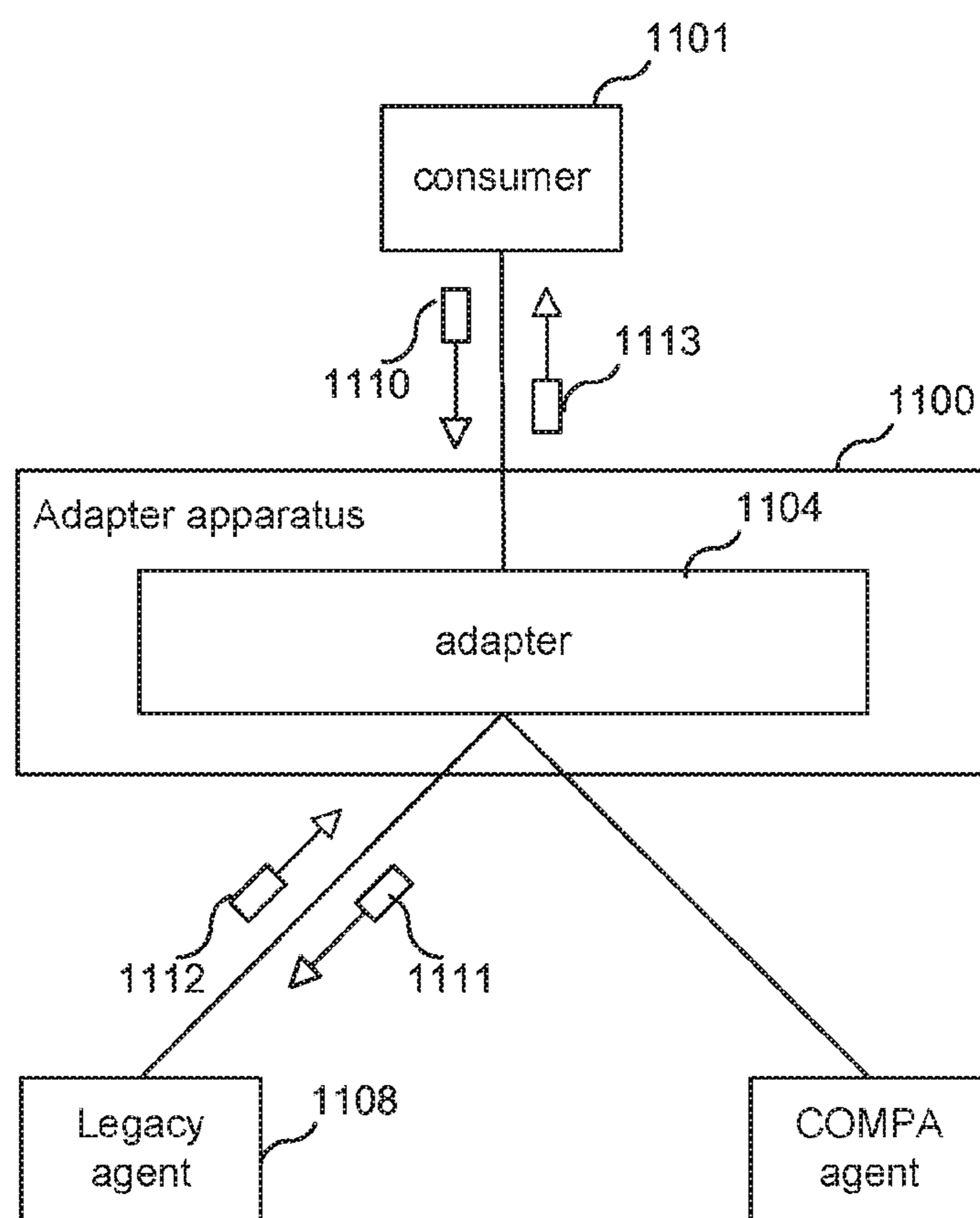


FIG. 11

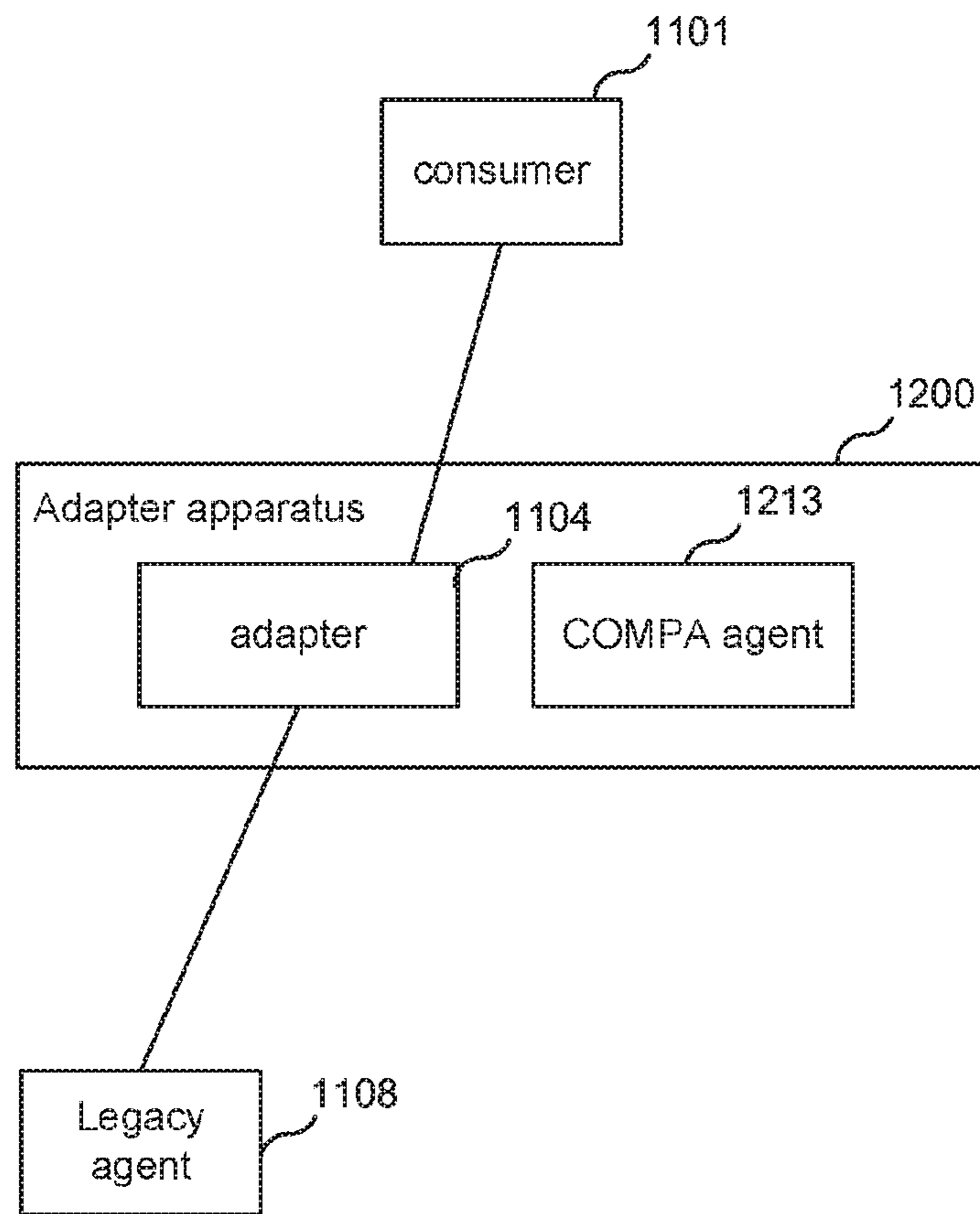


FIG. 12

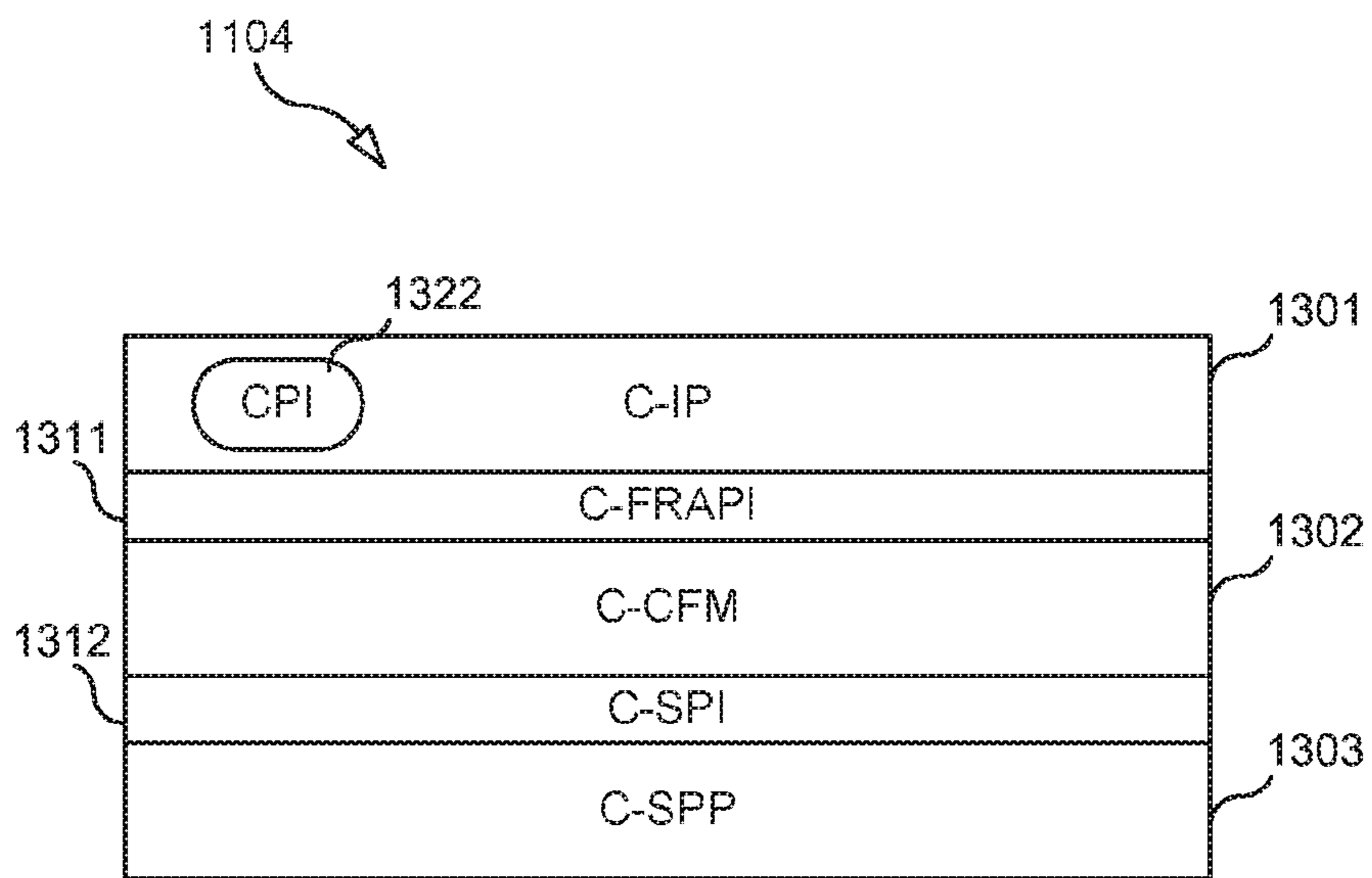


FIG. 13

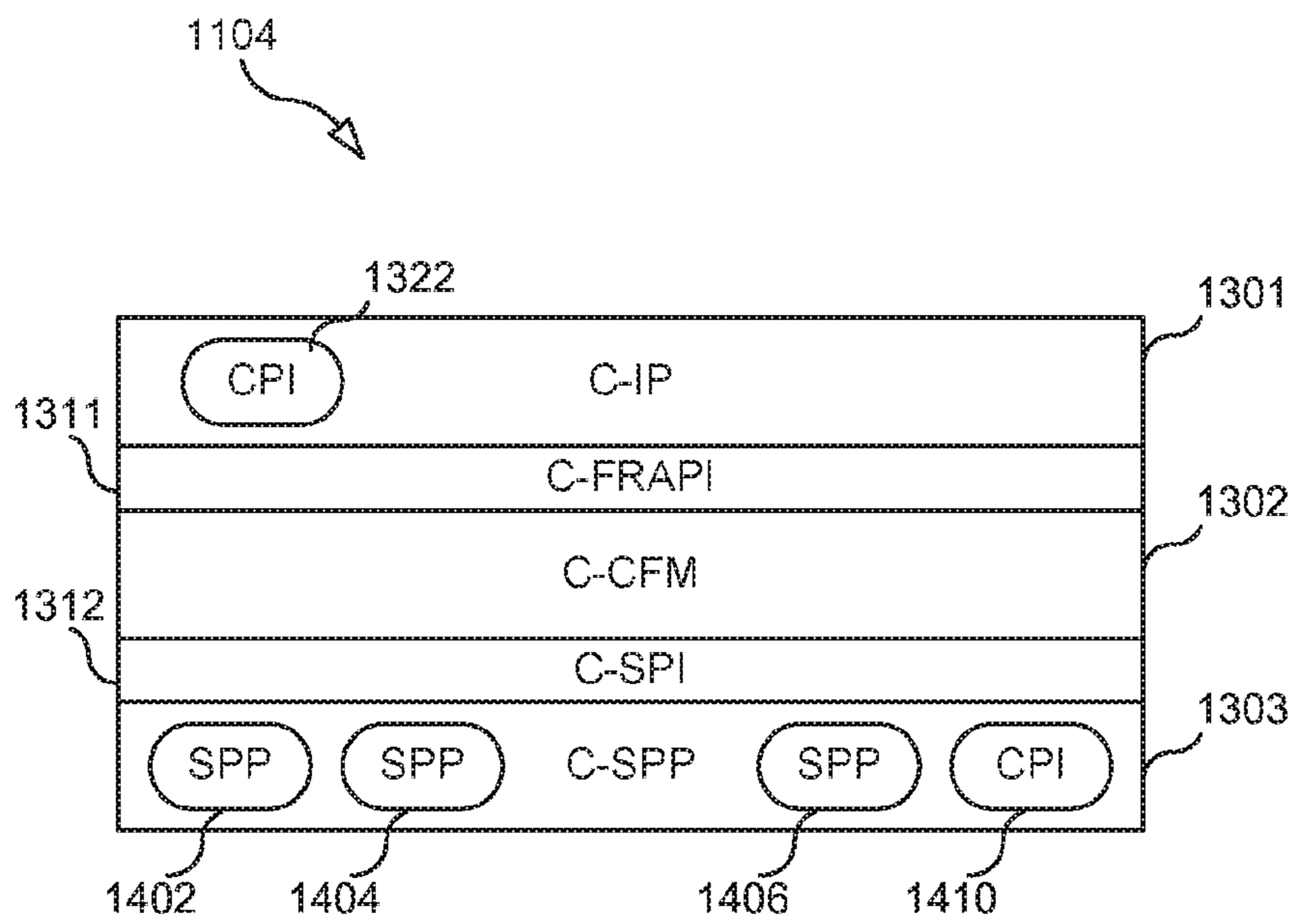


FIG. 14

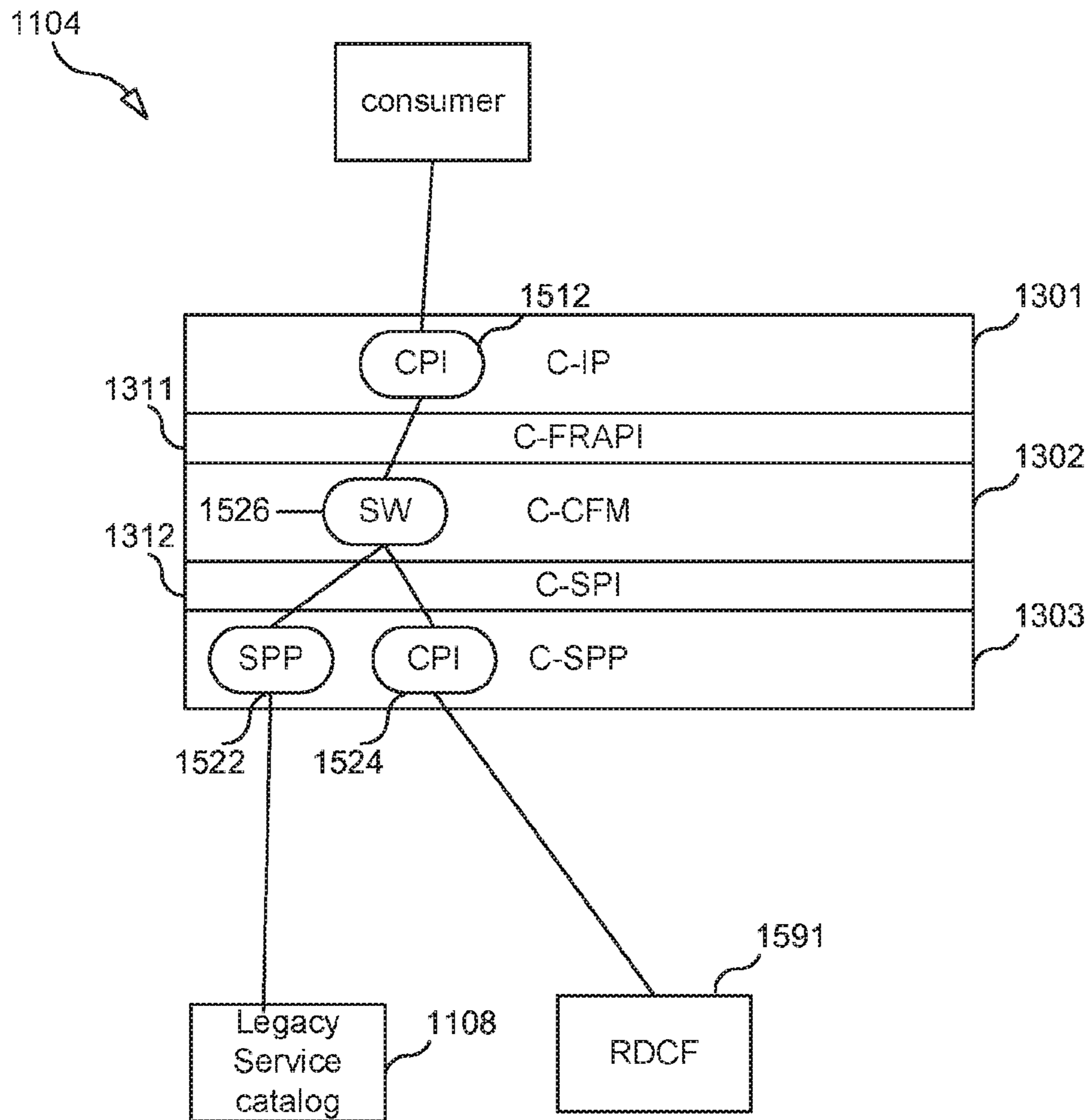


FIG. 15

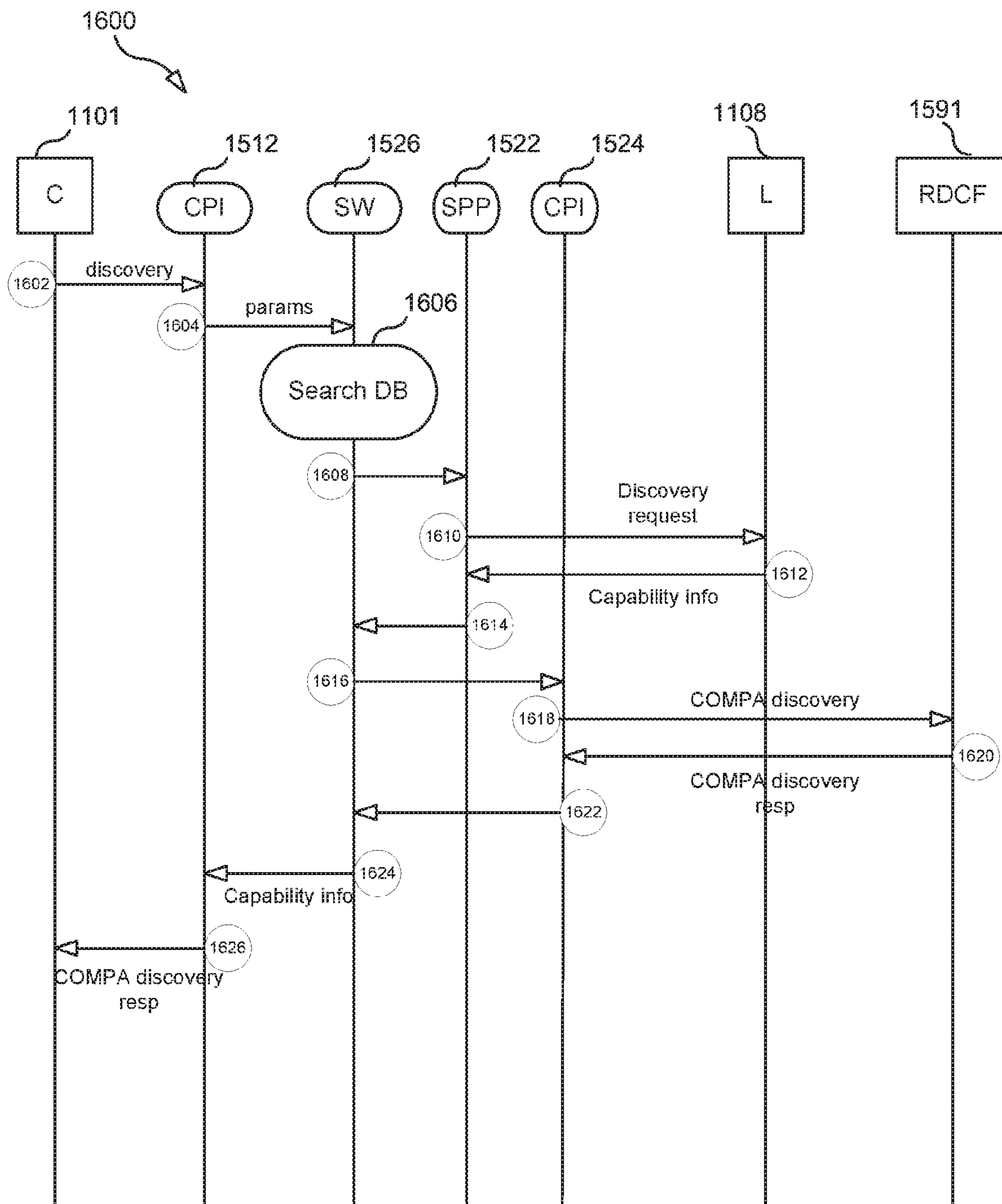


FIG. 16

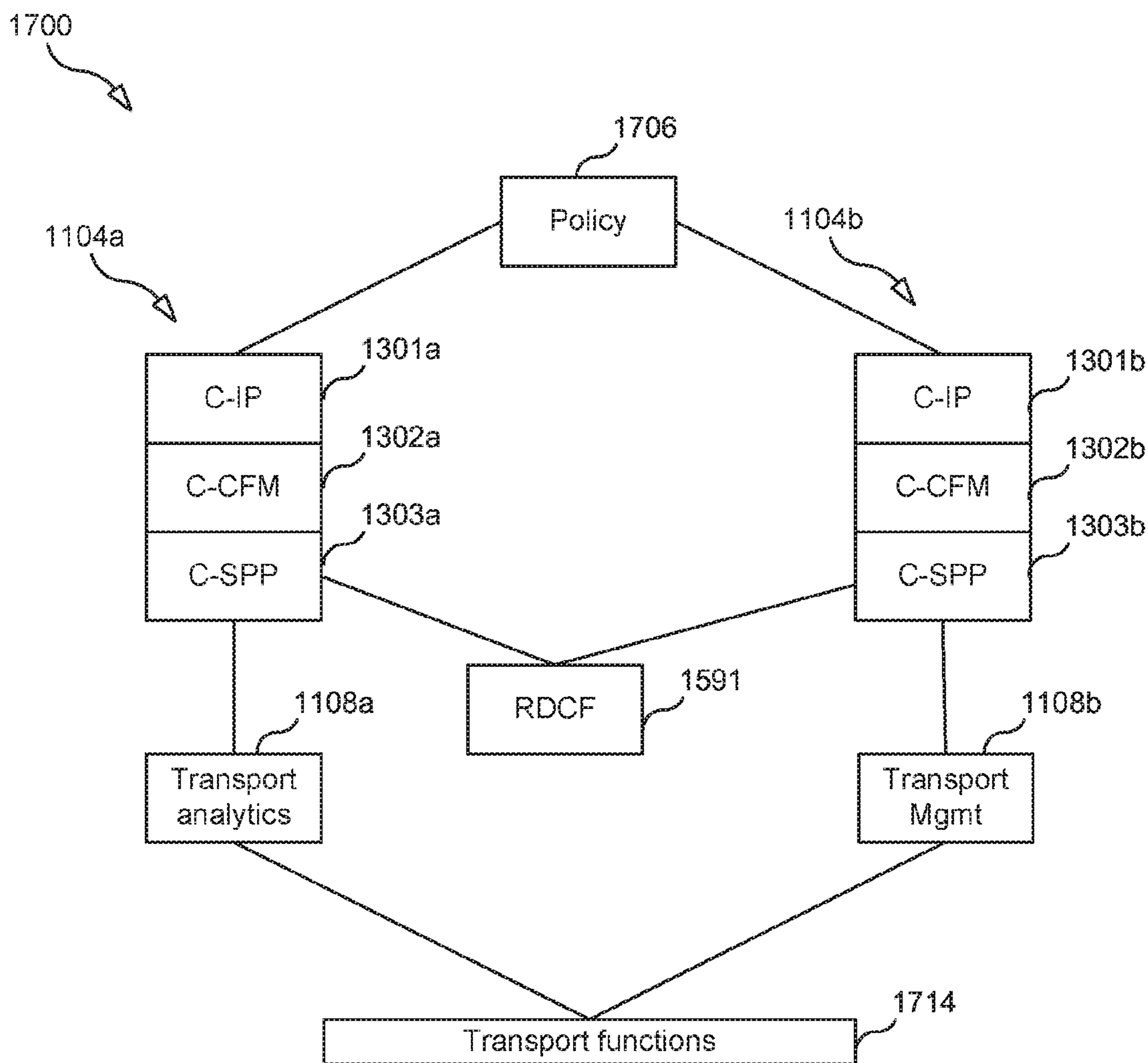


FIG. 17

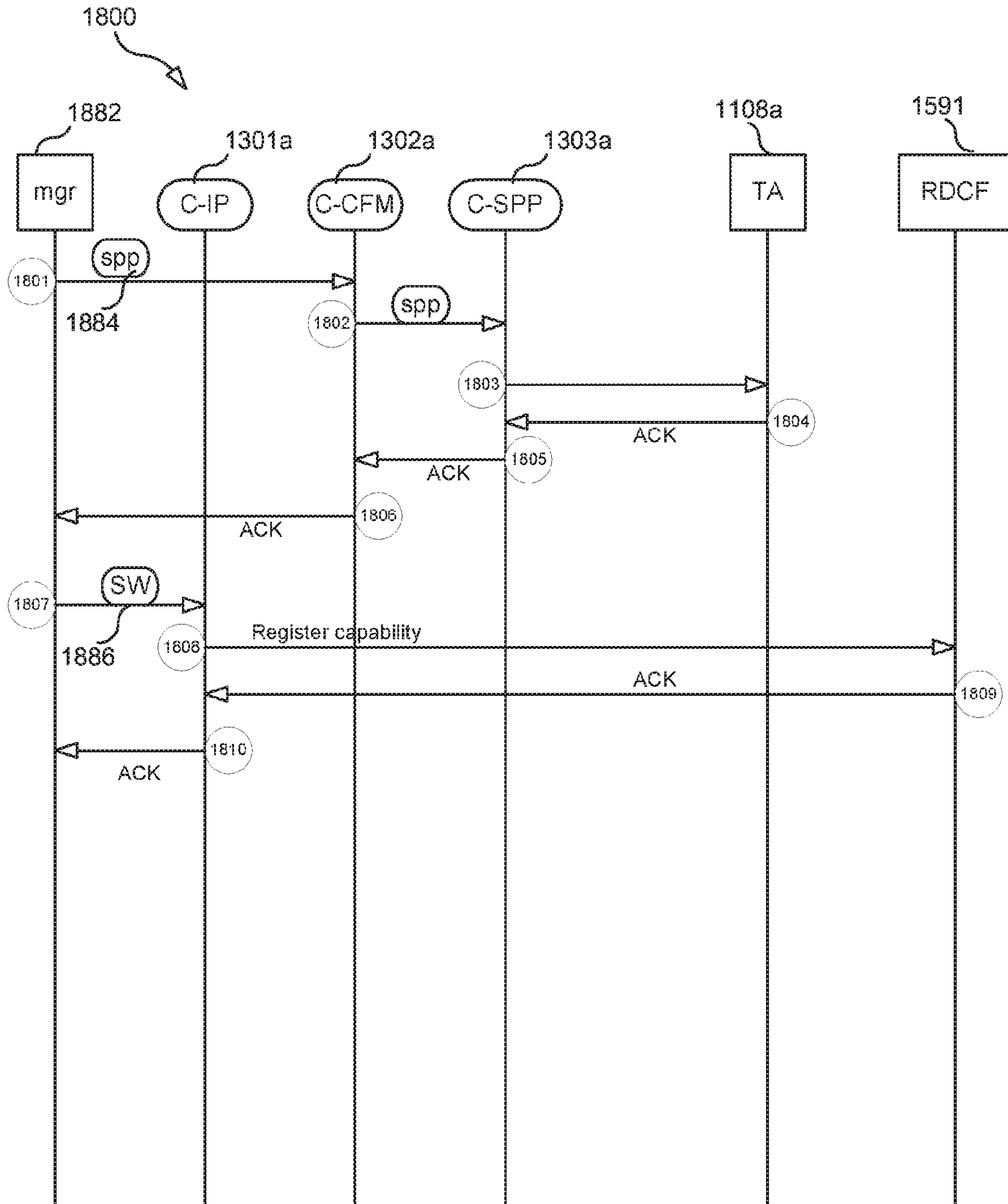


FIG. 18

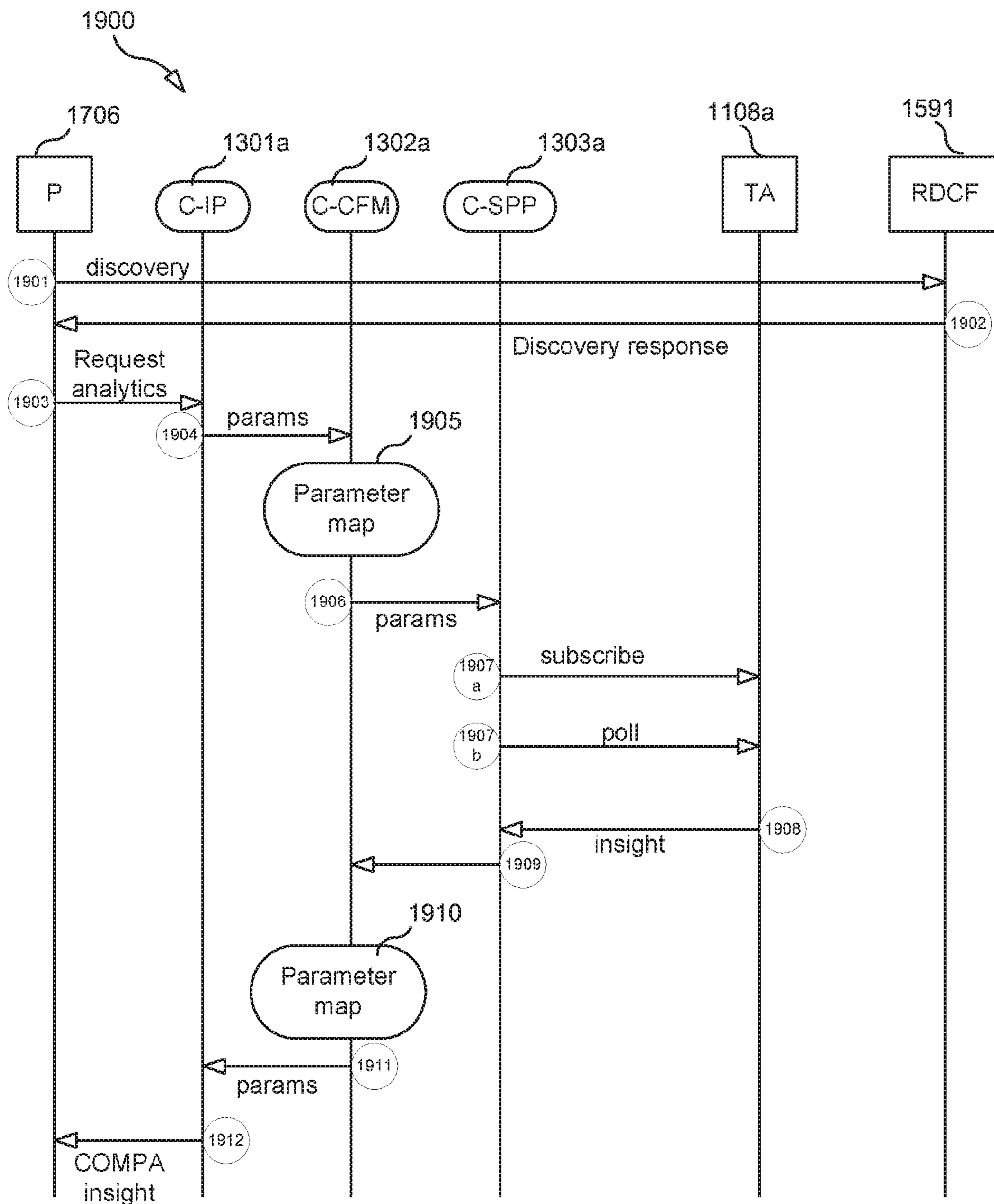


FIG. 19

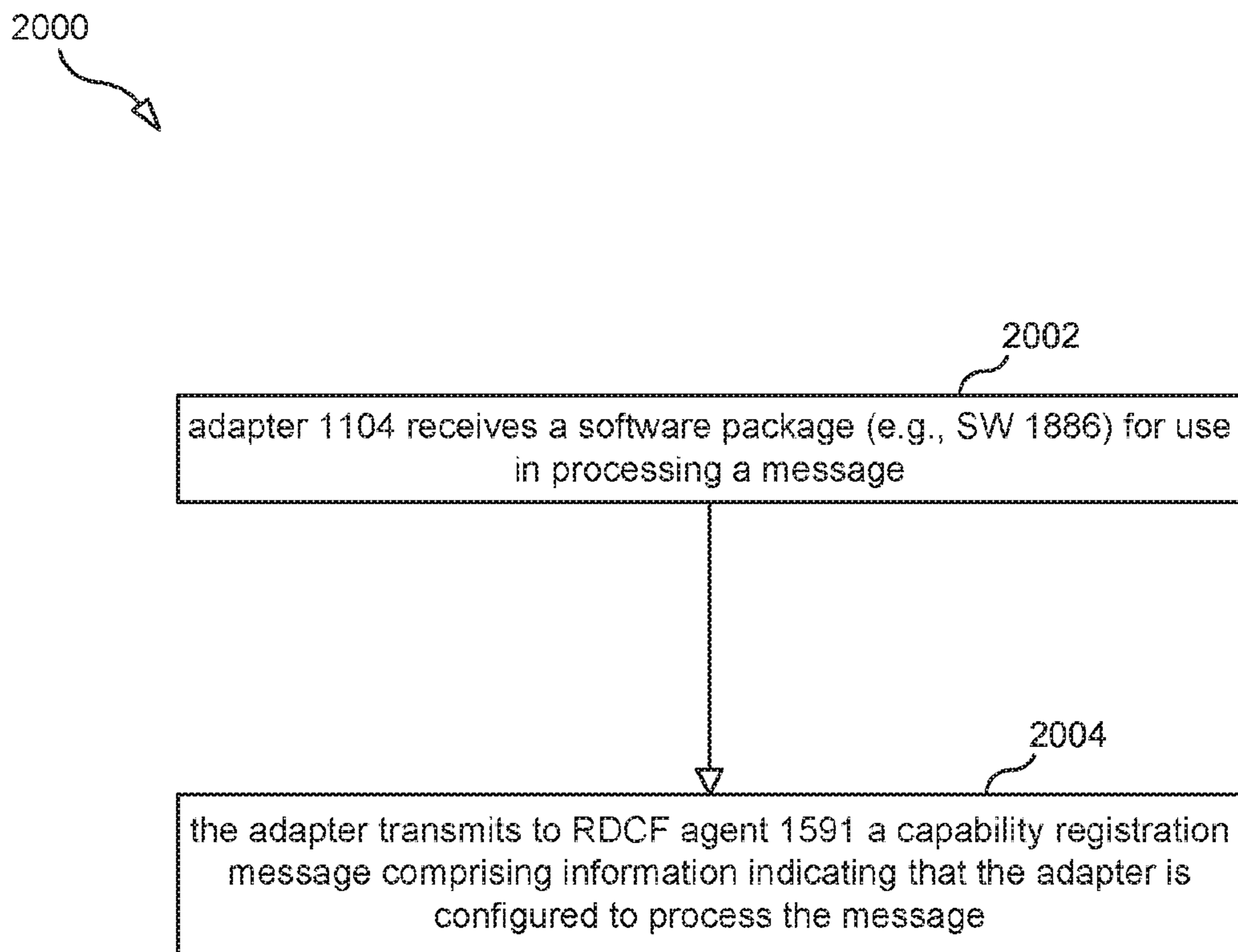


FIG. 20

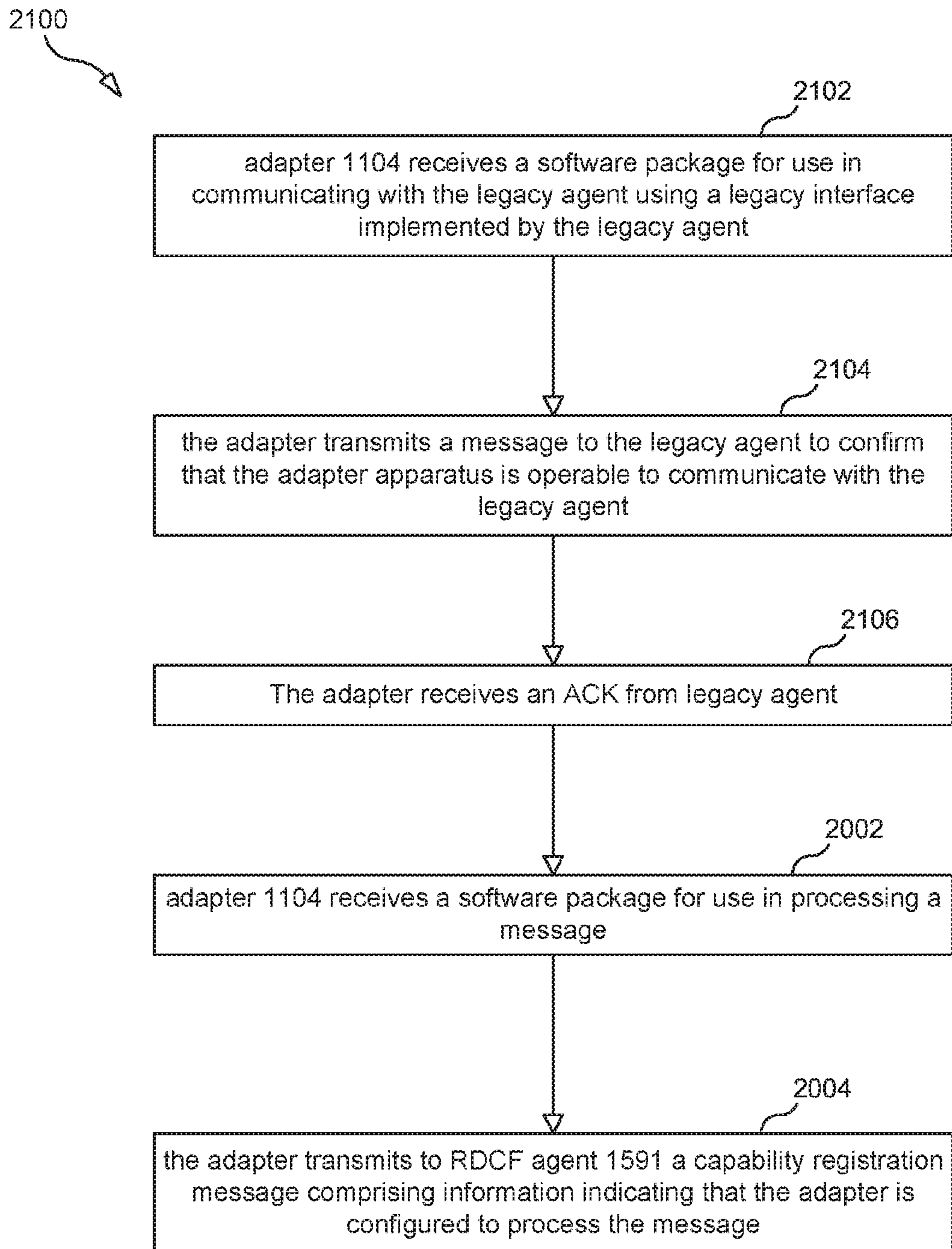


FIG. 21

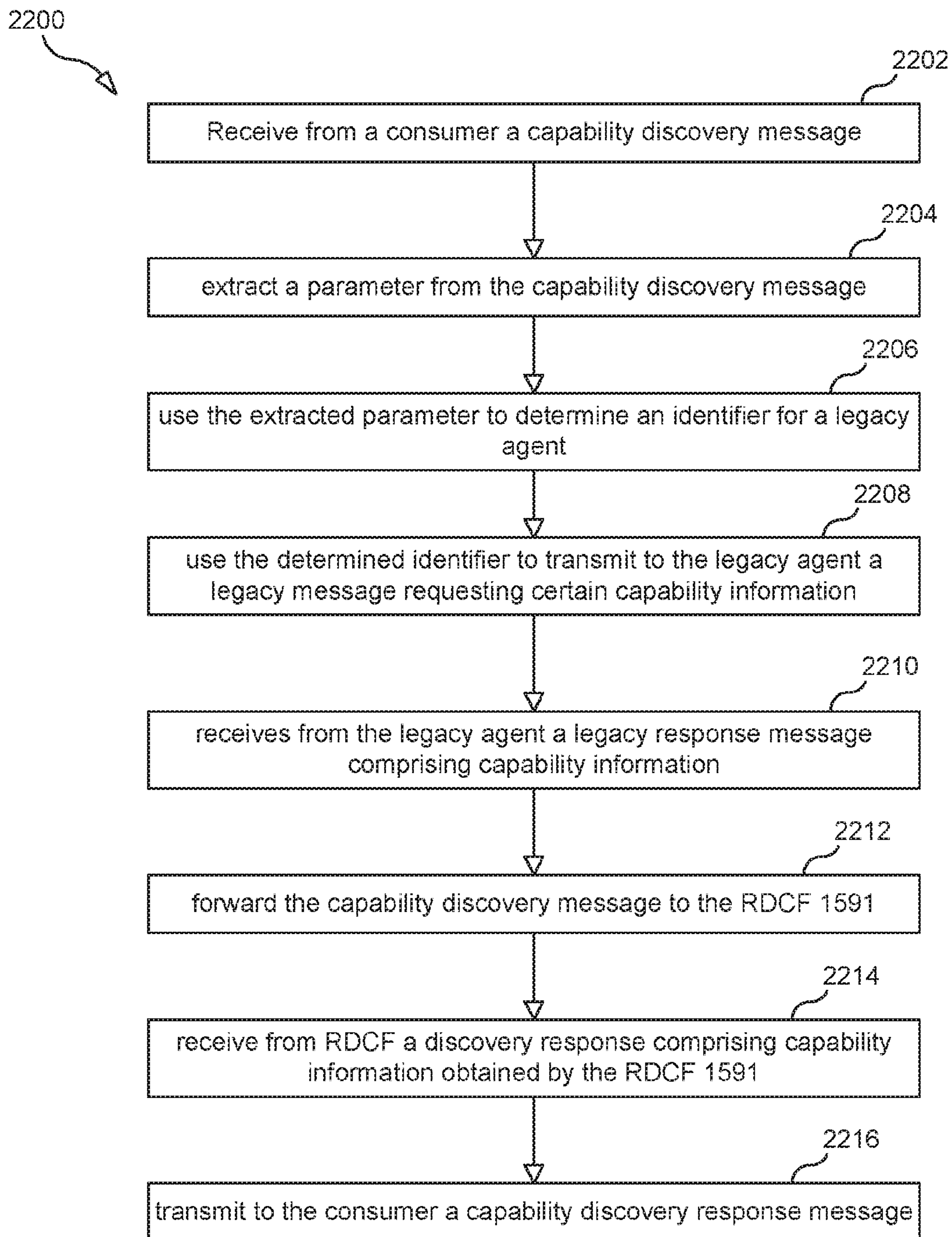


FIG. 22

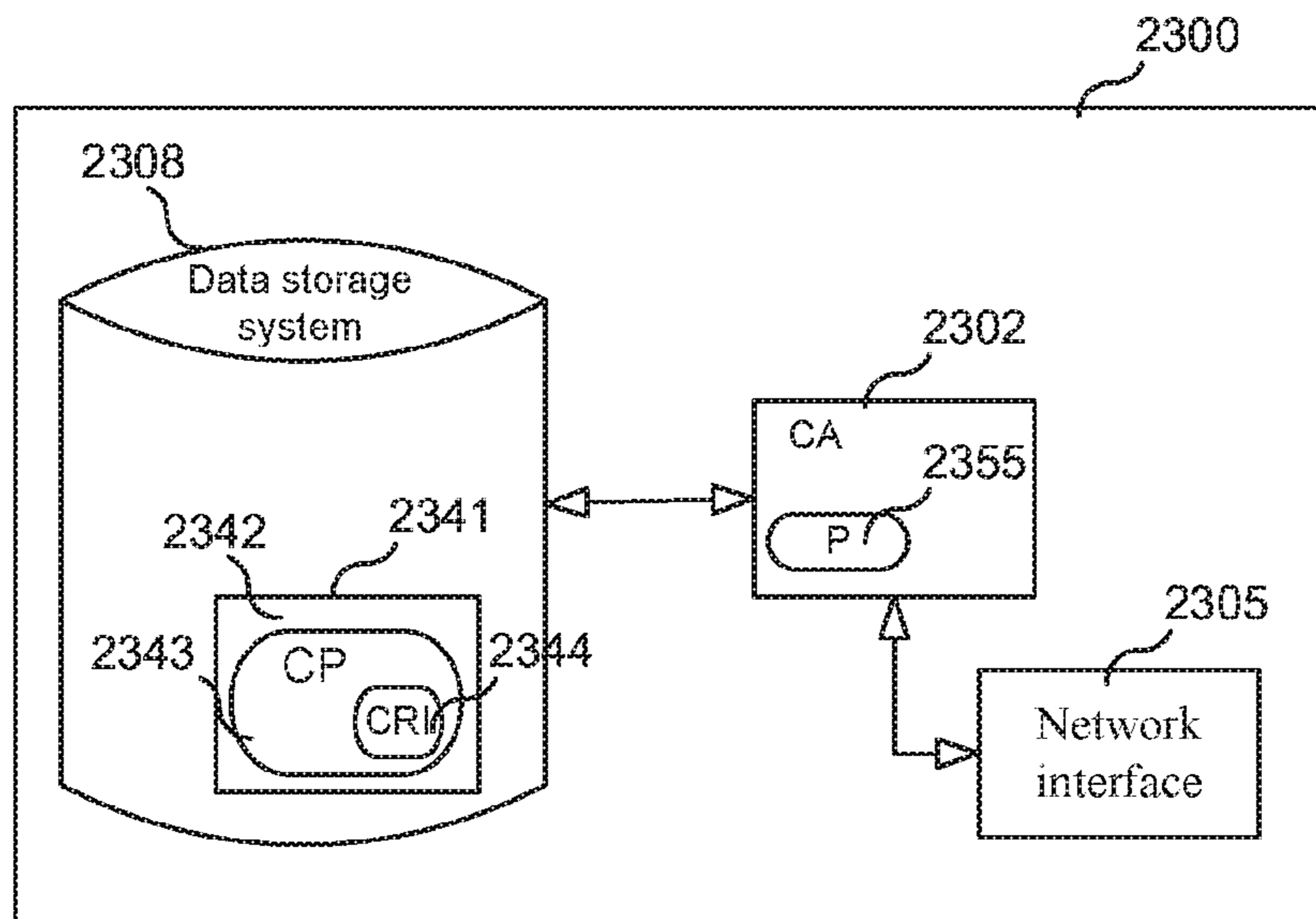


FIG. 23

AUTOMATIC NETWORK MANAGEMENT SYSTEM AND METHODS

CROSS REFERENCE TO RELATED APPLICATION(S)

This application is a 35 U.S.C. § 371 National Stage of International Patent Application No. PCT/SE2016/050724, filed Jul. 18, 2016, designating the United States and claiming priority to International Application No. PCT/SE2016/050659, filed on Jun. 29, 2016, which is incorporated by this reference.

TECHNICAL FIELD

Aspects of this disclosure relate to systems and methods for network management.

BACKGROUND

The goal of increasing the degree to which a network is managed automatically is not new. Autonomic networks have been a subject of research over the last 15 years, and technologies for achieving network automation are evolving. Recently there have been advances in a few specific technologies that increase both the urgency to increase automation as well as the possibilities of doing so. For example, Network Function Virtualization (NFV) provides flexibility in how network functionality is deployed and where it is deployed, which is enabled by the increasing maturity of cloud execution environments to support large number of diverse workloads in either a centralized or distributed manner. Additionally, Software Defined Networking (SDN) enables networking flexibility and the means to provide connectivity (networking) to the deployed virtual or physical network functions. This is often referred to as programmable networking. Furthermore, analytics technologies have evolved to the state where they can provide advanced insights about the state of the network.

SUMMARY

The increased flexibility provided by new technologies, such as SDN and NFV, has led to networks that are difficult to operate and require a high degree of manual intervention if continuing with the traditional approaches. Existing solutions to this problem tend to group together several functions to achieve a desired result. For example, existing solutions group together the means for producing insights (analytics), the means for selecting a recommended action based on insights (policy), and the means for executing the recommended actions. Some such existing solutions merely rely on a script to produce the insights, make the recommendations based on the insights, and then perform the recommended actions. Such scripts are rather inflexible and typically need to be manually modified in the event the recommended action does not produce the intended result or the inputs to the script change. Additionally, because such scripts tightly couple the implementation of the required functions it is very difficult to change one of the functions (e.g., analytics or policy) without a major impact.

Described herein is a network management architecture referred to as the Control, Orchestration, Management, Policy and Analytics (COMPA) architecture (or COMPA for short).

The COMPA architecture functions to simplify and automate the operations (both management and business pro-

cess) of a network. In one aspect, the COMPA architecture addresses four use case categories: (1) Resource/Service Onboarding; (2) Automated Product Offerings; (3) Automated Management; and (4) Service Exposure. COMPA enables rapid service introduction into the network and lifecycle management; dynamic network governance via policy; and controlled access to functionality provided by different responsibility domains.

In one embodiment, the COMPA architecture includes five COMPA agents that each provide a unique set of functionality. These five COMPA agents are: (1) a Control, Orchestration and Management (COM) agent; (2) a policy agent (P); (3) an analytics agent (A); (4) a Responsibility Domain Common Functions (RDCE) agent, and (5) a SAC agent. The features and functionality of these agents are further described in PCT/SE2016/050659.

In some embodiments, a network management system may employ one or more COMPA adapter agents. A COMPA adapter agent may be a standalone component of the network management system or it may be a component of any one of the described COMPA agents.

In one aspect, a COMPA adapter agent provides COMPA interfaces and COMPA framework procedures as an add-on to implementations of A, P, COM, RDCE, and SAC functionality. A COMPA adapter agent can be used for distributed and gateway service exposure realizations. The COMPA adapter agents can be used to adapt both existing or new non-COMPA implementations (a.k.a., "legacy" implementations) to a COMPA architecture (framework), and to build new COMPA adapted implementations.

[[insert claims]]

The above and other aspects and embodiments are described below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated herein and form part of the specification, illustrate various embodiments.

FIG. 1 illustrates a high level responsibility domain (RD) architecture according to some embodiments.

FIG. 2 illustrates components of a COMPA system according to some embodiments.

FIGS. 3-7 are message flow diagrams illustrating various processes according to some embodiments.

FIG. 8 is a flow chart illustrating a process according to some embodiments.

FIG. 9 is a flow chart illustrating a process according to some embodiments.

FIG. 10 is a flow chart illustrating a process according to some embodiments.

FIG. 11 illustrates an example adapter apparatus according to some embodiments.

FIG. 12 illustrates an example adapter apparatus according to other embodiments.

FIG. 13 illustrates a COMPA adapter agent according to some embodiments.

FIG. 14 illustrates a C-SPP layer of an adapter according to some embodiments.

FIG. 15 illustrates an example use case.

FIG. 16 is a message flow diagram illustrating a process according to some embodiments.

FIG. 17 illustrates another example use case.

FIG. 18 is a message flow diagram illustrating a process according to some embodiments.

3

FIG. 19. is a message flow diagram illustrating a process according to some embodiments.

FIG. 20 is a flow chart illustrating a process according to some embodiments.

FIG. 21 is a flow chart illustrating a process according to some embodiments.

FIG. 22 is a flow chart illustrating a process according to some embodiments.

FIG. 23 is a block diagram of a system for implementing one or more agents.

DETAILED DESCRIPTION

I. Responsibility Domains:

FIG. 1 illustrates a high level network architecture diagram of an example network 100 according to some embodiments. As illustrated in FIG. 1, the network 100 may be segregated into a number of Responsibility Domains (RD) as a way to provide separation of concerns. An RD corresponds to a set of functions under the responsibility of a specific organization within a network operator's business structure. The division of functions for a given RD is subject to the network operator's internal organizational structure and may change from network operator to network operator. Each RD will typically contain all the necessary functionality for the related organization to execute on its responsibility, and the functionality may be shared/replicated with other RDs. Each RD has the capability to expose services that can be consumed by others; and itself consumes services provided by other RDs, as explained herein.

As further shown in FIG. 1, the example network 100 is divided into five RDs: an Access RD, a Network Functions RD, a Cloud Infrastructure RD, a Transports RD, and Business and cross-domain operations RD. As further shown, each RD may implement its own COMPA system.

II. Exemplary COMPA System

FIG. 2 illustrates an exemplary COMPA system 200, which can be implemented in any one or more of the RDs shown in FIG. 1 or other RDs not illustrated. As shown in FIG. 2, the exemplary COMPA system 200 includes the following agents: an analytics agent 204, a policy agent 206, a COM agent 208 and an RDCF agent 202. Other COMPA system may consist of subsets of these agents and/or may include additional agents.

In some embodiments, COM agent 208 is configured to perform requested actions, such as, for example, actions requested by a policy agent and actions for supporting resource and service onboarding requests. Thus, in some embodiments, COM agent 208 is configured to receive action request messages that request COM agent 208 to perform actions, such as, for example, onboarding of resources and/or services.

In some embodiments, a resource can be any one of: a network agent (a.k.a., "network function")—e.g., Mobility Management Entity, Serving Gateway, etc., switching/routing equipment, computing resources, storage resources, a COMPA agent.

In some embodiments, policy agent 206 functions to request a COM agent, such as COM agent 208, to perform certain actions based on, for example, a policy decision that policy agent makes based on, for example, insights received from an analytics agent, such as analytics agent 202 or an analytics agent in another COMPA system in another RD. Accordingly, policy agent may be configured to transmit insight request messages to an analytics agent and transmit action request messages to a COM agent. Additionally, policy agent 206 may be configured to receive from a

4

COMPA system agent (e.g., a COM agent) or a non-COMPA system policy event messages that contain information for use by policy agent in making the policy decision.

In some embodiments, Analytics 204 agent is configured to provide insights (i.e., reports), such as insights identifying current (and/or predicted) events or conditions within the network. For example, in some embodiments, analytics agent 204 is configured such that, in response to receiving a historical insight request message, analytics agent 204 periodically transmits an historical insight to the requesting entity, which is typically a policy agent, and is further configured such that, in response to receiving a real-time insight request message, analytics agent 204 immediately transmits an insight to the requesting entity.

In some embodiments, RDCF agent 202 provides service exposure, maintains catalogs (e.g., a service catalog and/or a resource catalog), and maintains inventories.

A. Analytics Agent 204 Messages

As explained above, analytics agent 204, in some embodiments, is configured to act on certain defined COMPA Analytics messages. In some embodiments, these COMPA Analytics messages include the following messages: 1) the historical insight request message; 2) the real-time insight request message; 3) an historical insight tuning message; and 4) an historical insight termination message. The below tables (Tables 1-4) illustrate the information elements that may be included in each of the messages:

TABLE 1

historical insight request message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Periodicity	Specifies the time interval for reporting, i.e., how often reports should be generated (e.g., at a certain time of day or as soon as an insight report is available).
Report Type	Continuous reporting or specific report (requested with ID). A request for a specific report overrides periodicity.
Delivery Type	The requested type of delivery of the insight report: e.g., guaranteed delivery ("Class1"), non-guaranteed delivery ("Class4"), Error-detection delivery ("Class2")
Insight Object	Specifies the target for the analytics, e.g. per subscriber, group of subscribers, network element, etc.
Requested Insight Type	The requested type of analytics chosen from the list of supported insight types e.g., the insights available e.g., for security-analytics, roaming-analytics, transport network analytics, churn analytics
Request Insight Type Qualifier	This parameter is a container and allows a consumer to specify options available for a Requested Insight Type. Examples are: "Insight Quality Selection" (High, Medium, Low), "Insight Type Option Selection" (e.g., roaming analytics with or without usage data). The available options are obtained with the service Capability discovery procedure.

TABLE 2

real-time insight request message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added).
Delivery Type	The requested type of delivery of the insight report: e.g., guaranteed delivery ("Class1"), non-guaranteed delivery ("Class4"), Error-detection delivery ("Class2")

5

TABLE 2-continued

real-time insight request message	
Information Element	Description
Insight Object	Specifies the target for the analytics, e.g., per subscribers, a group of subscribers, network element, etc.
Requested Insight Type	The requested type of analytics chosen from the list of supported insight types e.g., the insights available e.g., for security-analytics, roaming-analytics, transport network analytics, churn analytics
Requested Insight Type Qualifier	This parameter is a container and allows a consumer to specify options available for a Requested Insight Type. Examples are: "Insight Quality Selection" (High, Medium, Low), "Insight Type Option Selection" (e.g., roaming analytics with or without usage data). The available options are obtained with the Service Capability discovery procedure.

TABLE 3

historical insight tuning message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added).
Delivery ID	Handle identifying the Analytics Insight Delivery instance.
Tune Historical	A container for parameters specifying the historical insight delivery also used in the "Request Historical Analytics Insight Delivery" operation; e.g., Periodicity, Report Type, Delivery Type, Insight Object, Requested Insight Type and Requested Insight Type Qualifier. See Request Historical Analytics Insight Delivery for further information.
Tune Real-Time	A container for parameters specifying the real-time insight delivery also used in the "Request Real-Time Analytics Insight Delivery" operation: e.g., Delivery Type, Insight Object, Requested Insight Type Requested and Insight Type Qualifier. See Request Real-Time Analytics Insight Delivery for further information. This parameter is used to add historic analytics (trend insights) as input to the real-time analytics job.

TABLE 4

historical insight termination message	
Information Element	Description
Version	Specifies the version of the operation
Delivery ID	Handle identifying the Analytics Insight Delivery Instance.

With respect to the historical insight request message, as a result of receiving this message, analytics agent **204** creates in a database a record storing information contained in the received message (e.g., the periodicity, report type, etc.) and transmits to the entity that transmitted the request an acknowledgement message containing a delivery identifier for use in later retrieving the database record from the database. Also, as a result of receiving the historical insight request message, analytics agent **204** will, based on the periodicity defined in the request, periodically transmit an historical insight delivery message comprising an insight. The transmitted historical insight delivery message may further include the identifier that was included in the acknowledgement message. The insight included in the

6

historical insight delivery message may be formatted using a markup language (e.g., Extensible Markup Language (XML)) or using JavaScript Object Notation (JSON)) or otherwise formatted.

With respect to the historical insight tuning message, as a result of receiving this message, analytics agent uses the delivery identifier included in the tuning message to update the database record based on the parameters included in the tuning message (e.g., the periodicity parameter).

With respect to the historical insight termination message, as a result of receiving this message, analytics agent uses the delivery identifier included in the tuning message to delete the database record or update the database record to indicate that no further historical insights defined by the record should be sent.

With respect to the real-time insight request message, as a result of receiving this message, analytics agent **204** generates a real-time insight and transmits a real-time insight delivery message comprising the generated real-time insight. In some embodiments, after the insight request message is received and before the delivery message is sent, analytics agent **204** transmits an acknowledgement message with a delivery identifier, and the delivery message includes the delivery identifier. The insight report may be formatted using XML or JSON and contains information (e.g., real-time information) requested in the real-time insight request message.

B. Policy Agent **206**

Policy agent **206**, in some embodiments, is configured to act on certain defined COMPA Policy messages. In some embodiments, these COMPA Policy messages include: 1) a policy data message; and 2) request policy decision message. The below tables (Tables 5 and 6) illustrate the information elements that may be included in each of the messages:

TABLE 5

Policy Data Message	
Information Element	Description
Version	Specifies the version number of the message
Event Report (required)	Information that the policy agent may use in making a policy decision
Context	Additional information that the policy agent may use in making a policy decision

TABLE 6

Request Policy Decision Message	
Information Element	Description
Version	Specifies the version number of the message
Policy Decision Input	Parameters required for execution of a policy statement (e.g., rule) by the policy agent. These parameters may include a rule identifier to identify a rule that the policy agent should evaluate
Context	Additional information that the policy agent may use in making a policy decision

With respect to the policy data message, this message can be transmitted to the policy agent by any resource in the network. As a result of receiving this message, policy agent **206** may store the event report (or stores at least some of the information included in the event report) so that the information can be used at a later time as input to a policy statement executed by policy agent **206**, or policy agent may execute a policy statement based on the event report immediately after receiving the policy data message. As one example, a resource (e.g., a security system which may or may not follow COMPA principles) sends a policy data message to the policy agent with an event report containing information informing the policy agent about a detected denial of service attack, and the policy agent acts on this information immediately by, for example, determining based on a policy statement a set of or more actions that should occur.

With respect to the request policy decision message, as a result of receiving this message, policy agent **206** uses the information contained in the Policy Decision Input IE (and possibly previously stored event report information) to execute a policy statement, and thereby make a policy decision. An identifier identifying the policy statement may be included in the Policy Decision Input IE together with parameters required by the policy statement. In some embodiments, the result of the policy decision is returned to the entity that transmitted the request policy decision message.

In some embodiments, as a result of executing a policy statement, the policy agent may be triggered to send to a COM agent a Request Action message.

C. COMAgent **208**

COM agent **208**, in some embodiments, is configured to act on certain defined COMPA COM messages. In some embodiments, these COMPA COM messages include the messages identified in TABLE 7.

TABLE 7

Messages COM Agent is configured to Act On	
Message Name	COM agent Response
Request Action	performs action identified in the request using action parameters, if any, included in the request. COM agent, after performing the action, may transmit to the entity sending the request (usually a policy agent), a requested action outcome report specifying the result of the action (e.g., Success or failure) and an action ID for identifying the action
Deploy Resource Specification	deploys the descriptions of the resource and the resource SW.
Delete Resource Specification	deletes the descriptions of the resource and the resource SW.
Deploy Service Specification	deploys the descriptions of the service.
Update Service Specification	updates the descriptions of an already deployed service.
Delete Service Specification	deletes the descriptions of the service.
Instantiate Resource	instantiates a resource, or change an already instantiated resource (e.g. deploy/activate the resource SW)
Release Resource Instance	releases a resource instance i.e. reducing the capacity of the resource type. The request also includes how the potential used sub-resources should be handled.
Instantiate Service	instantiates a service based on a deployed service i.e. descriptions are already available including the descriptions of the resources needed for the services type, hence applicable resource instantiation will happen. Or request to change an already instantiated service.
Release Service Instance	releases a service instance i.e. reducing the capacity of the service type. The request also includes how the used resources should be handled.

Tables 8 to 17 below illustrate an exemplary embodiment of the COM agent messages shown in table 7.

TABLE 8

Request Action Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Action	Specifies the action that the COM agent is being asked to perform.
Action parameters	Additional parameters, depending on action.

TABLE 9

Deploy Resource Specification Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Resource Descriptor	Contains all aspects of the resource e.g. the description of and the requirements of the resource. This should either be the object or the reference to where the object can be found.
Resource SW	The software package (SW), if any, for implementing the resource or a pointer to the SW. The SW contains executable software (e.g., scripts, executable binary code (e.g., OVF image), etc.)

9

TABLE 10

Delete Resource Specification Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Resource Specification ID	The identity of the resource specification to be deleted.

TABLE 11

Deploy Service Specification Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Service Descriptor	Contains all aspects of the service e.g. the description of and the requirements of the service e.g. needed resources. This should either be the object or the reference to where the object can be found.

TABLE 12

Update Service Specification Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Service Specification ID	The identity of the service specification to be updated.
Service Descriptor	Contains all aspects of the service e.g. the description of and the requirements of the service e.g. needed resources. This should either be the object or the reference to where the object can be found.
Instantiated Services handling	Defines if the already instantiated services based on this Service Specification ID should be updated based on this service update

TABLE 13

Delete Service Specification Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Service Specification ID	The identity of the service specification to be delete.

TABLE 14

Instantiate Resource Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Identity	Identity of the resource specification to be instantiated, or the instantiated resource to be changed identified with Resource Specification ID and Resource Instance ID, respectively
Context	Contains the context in which a resource specification should be instantiated e.g. capacity, affinity,

10

TABLE 14-continued

Instantiate Resource Message	
Information Element	Description
	configuration including how, when and by who the instantiated resource can be used, or the changed context of an already instantiated resource.

TABLE 15

Release Resource Instance Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Resource Instance ID	The identity of the instantiated resource to be released.
Sub resource management	Specifies how possible resources used by this instantiated resource should be handle e.g. released or kept.

TABLE 16

Instantiate Service Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Identity	Identity of the service specification to be instantiated, or the instantiated resource to be changed identified with Service Specification ID and Service Instance ID, respectively.
Service Parameters	parameters to tailor the service, these could be service level parameters such as addressing information, or it could be parameters that influence the characteristics of the service.
Context	Contains the context in which a service specification should be instantiated e.g. capacity, affinity, configuration including how, when and by who the instantiated resource can be used, or the changed context of an already instantiated service.

TABLE 17

Release Service Message	
Information Element	Description
Version	Specifies the version of the operation (RD name may be added)
Service Instance ID	The identity of the instantiated service to be released.
Resource management	Specifies how the resources used by this instantiated service should be handle e.g. released or kept.

D. RDCF Agent 202

RDCF agent 202, in some embodiments, is configured to act on certain defined COMPA RDCF messages. In some embodiments, these COMPA RDCF messages include the messages identified in table 18 below.

TABLE 18

Message	RDCF agent response
C_Service Capability Registration	Registers both specification and instances of services/resources supplied by the invoker (e.g., A, P, and COM)
C_Service Capability Discovery	Searches for a matching Service Capability and if found transmits a C_Service Capability Discovery Response
C_Service Capability Delete	Removes a Service Capability identified in the message
C_Service Capability Update	Updates both specification and instances of the identified service capability
Service Specification Registration	Stores a service specification containing the service description included in the message
Service Specification Discovery	Searches for requested service specification and if found returns a reference to the matching registered service specifications URI.
Service Specification Delete	Removes the identified service specification
Service Specification Update	Updates the identified service specification
Services Instance Registration	Registers the identified service instance (e.g., stores information included in the message in a service instance registration record).
Service Instance Discovery	Searches for an instance of the specified service type and if found return an identifier for the instance (e.g., a reference to the matching registered services, URI).
Service Instance Delete	Removes the identified service instance
Service Instance Update	Updates the identified service instance (e.g., updates the a service instance registration record for the service)
Resource Specification Registration	Stores a resource specification containing the resource description included in the message
Resource Specification Discovery	Searches for requested resource specification and if found return a resource specification id.
Resource Specification Delete	Removes the identified resource specification
Resource Specification Update	Updates the identified resource specification
Resource Instance Registration	Registers the identified service instance (e.g., stores information included in the message in a resource instance registration record).
Resource Instance Discovery	Searches for an instance of the specified resource type and if found return an identifier for the instance
Resource Instance Delete	Removes the identified resource instance
Resource Instance Update	Updates the identified resource instance (e.g., updates the a resource instance registration record for the resource)
Authentication Validation	Validates the credentials included in the message
Authorization Validation	Verifies that an authenticated entity consumer has the correct permissions and rights to access the requested operation

Tables 19-40 illustrate the information elements that may be included in each of the messages show in TABLE 18.

TABLE 19

C_Service Capability Registration	
Information Element	Description
Version	Specifies the version of the operation
C_Service Capability ID	Specifies the COMPA capability to be registered (e.g., a Policy capability or an Analytics capability).
Address	Address for the service (e.g., IP address, server name, URL, URI, URN). This address is used by a consumer when requests a service e.g.- "Request Historical Analytics Insight Delivery".
Service Description	Identifies the type of service capability that is registered with a description of the service, e.g., Service Operations, Service Parameters, Service Meta data etc. Each of the interfaces has an address (URN) for downloading interface specifications and a procedural description in text.

TABLE 20

C_Services Capability Discovery	
Information Element	Description
Version	Specifies the version of the operation
Requested Service	Request to obtain COMPA service description for all registered services, or for a specific type of service such as Analytics, Policy or COM

TABLE 21

C_Service Capability Delete	
Information Element	Description
Version	Specifies the version of the operation.
C_Service Capabilities	Specifies the key of COMPA capability to be Deleted.

13
TABLE 22

C_Service Capability Update Operation	
Information Element	Description
Version	Specifies the version of the operation.
C_Service Capabilities	Specifies the key of COMPA capability to change state.
Service Description	Identifies the attributes of service capability to be updated that is registered with description of the service, e.g., Service Operations, Services Parameters, Service Meta data etc. Each of the interfaces has an address (URN) for downloading interface specification and a procedural description in text.

TABLE 23

Service Specification Registration	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of network service to be registered
Service Description	Identifies the types of network service that is registered with a description of the service. Describes the type, operations, and parameters. These services are exposed over the native interfaces.
State	Defines the state in the lifecycle, e.g. Testing, Staging, Operational, Phase out, Retired.

TABLE 24

Service Specification Discovery	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the ID of network service to be discovered
Services Description	Describes the type of service to search for e.g., Describes service type, operations and parameters that matches.
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired to be matched

TABLE 25

Service Specification Delete	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of network services to be Deleted

TABLE 26

Service Specification Update	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of network service

TABLE 26-continued

Service Specification Update	
Information Element	Description
Service Description	Identifies the parameters of the specification to be updated and their new values. Describes service type, operations and parameters. These services are exposed over the native interface.
State	Defines the new state in the lifecycle, e.g. Testing, Staging, Operational, Phase out, Retired.

TABLE 27

Service Instance Registration	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type (specification) of the instance of the service to be registered. The specification must exist prior to registering the instance of it.
Service Instance ID	Specifies the instance ID of service to be registered.
Address	URI for the service (This is in line with SOA architecture and corresponds to the address of service access point, targeting the service itself or a load balancer in front of the service itself. It does not directly correspond to the TMP SID information model where the service is "virtual"(independent of the implementation in a resource) and the actual "service access point" is found in the resource layer, linked by the resource facing service as a part of the service.)
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 28

Service Instance Discovery	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of service to be searched for.
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 29

Service Instance Delete	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of service instance to be Deleted.

TABLE 30

Service Instance Update	
Information Element	Description
Version	Specifies the version of the operation
Service Specification ID	Specifies the type of service instance to be updated.

15

TABLE 30-continued

Service Instance Update	
Information Element	Description
Service Instance ID	Identifies the Service Instance to be updated.
Service Instance	identifies the parameters of the instance entity to be updated in their new values.
State	Defines the new state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 31

Resource Specification Registration	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of network Resource to be registered
Resource Descriptor	Contains all aspects of the resource e.g. the description of and the requirements of the resource. This should either be the object or the reference to where the object can be found.
Resource SW	The software package (SW), if any, for implementing the resource or a pointer to the SW. The SW contains executable software (e.g., scripts, executable binary code (e.g., OVF image), etc.)
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 32

Resource Specification Discovery	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of network Resource to be discovered
Resource Description	Describes the type of Resource to search for, e.g., Resource Type, operations and parameters.
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 33

Resource specification Delete	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of network Resource to be Deleted

TABLE 34

Resource Specification Update	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of network Resource

16

TABLE 34-continued

Resource Specification Update	
Information Element	Description
Resource Specification	Identifies the parameters of the specification to be updated and their new values. Describes service type, operations and parameters. These services are exposed over the native interfaces.
State	Defines the new state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 35

Resource Instance Registration	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type (specification) of the instance of the resource to be registered. The specification must exist prior to registering the instance of it.
Resource Instance ID	Specifies the instance ID of Resource to be registered.
Address	URI for the resource
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 36

Resource Instance Discovery	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of resource instance to be searched for.
State	Defines the state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 37

Resource Instance Delete	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of resource instance to be Deleted.

TABLE 38

Resource Instance Update	
Information Element	Description
Version	Specifies the version of the operation
Resource Specification ID	Specifies the type of resource instance to be updated.
Resource Instance ID	Specifies the type of resource instance to be updated.
Resource Instance	Identifies the parameters of the instance to be updated and their new values.

17

TABLE 38-continued

Resource Instance Update	
Information Element	Description
State	Defines the new state in the lifecycle, e.g., Testing, Staging, Operational, Phase out, Retired.

TABLE 39

Authentication Validation	
Information Element	Description
Credentials	A consumer must have a valid consumer account configured by the administrator of the SAC database that specifies the consumer's permissions and rights. Consumer credentials must be associated with this account. Credentials may include user name + password, certificates, tokens, etc.
Session ID	Session ID
Time (optional)	This time validation against the timestamp that the SAC has stored for this user and session

TABLE 40

Authorization Validation	
Information Element	Description
Authenticated Consumer Identity	The consumer identity is related to the consumer credentials and are validated in the SAC.
Server ID	Server ID
Operation	This could be any of the operations provided by the COMPA interfaces C1-C4

Table 41 below illustrates an exemplary embodiment of the C_Service Capability Discovery Response.

TABLE 41

C_Service Capability Discovery Response	
Information Element	Description
C_Service Capability ID	Specifies the ID of capability to be discovered. In COMPA we have Analytic, Policy and COM but other capabilities may also use the same capability registration.
Address	URN for a service. This address is used by consumers of discovered services when these invoke a service, e.g., - "Request Historical Analytics Insight Delivery"
Services Description	Identifies the type of service capability that is registered with a description of the service, e.g. Service Operations, Service Parameters, Service Meta data etc. Each of the interfaces has an address (URN) for downloading interface specifications and a procedural description in text. Here the Service Description is used for finding matching entities.

In some embodiments, each of the messages described herein may further include a "token" information element as show below in table 42.

18

TABLE 42

Token IE	
Information Element	Description
token	Optional. Token is obtained after a successful authentication.

III. Use Case Categories

There are numerous possible uses cases for the COMPA system. In some embodiments, each use case can be categorized into one of the following four categories: Resource/Service Onboarding; Automated Product Offering (APO); Automated Management (AM); and Service Exposure (SE).

A. Resource/Service Onboarding:

In some embodiments, before a product (i.e., service) can be offered automatically using COMPA, the service and the resources required by the service must first be onboarded, which means that the specification for the service and the specification for each resource required by the service must be registered with an RDCF agent. This is referred to as Resource/Service Onboarding. Additionally, the resources required to instantiate the service must be instantiated (i.e., made operational) in response to a request to instantiate the service or must have been previously instantiated. That is, some resources will be instantiated when the service is instantiated (e.g. setting up a new network for a special type of service, how to setup the resources is not known before the service request is received), while other Resources that were instantiated before the request to instantiate the service is received may require a re-configuration for the service when the service is instantiated. Some resources will be also instantiated during operation to add more resources to cover an increase in load.

Resource/Service Onboarding includes: the deployment of service and resource specifications and the deployment of some resource instances. A service specification describes the services offered by the service and the elements (e.g., resources) that are needed in order for the service to provide the services the service offers. Accordingly, in some embodiments, service specifications identify (e.g., contain links to) resource specifications. Accordingly, in some embodiments, before a particular service specification is deployed, the resource specification identified by the particular service specification should be deployed first, if they are described as required to be instantiated in order to later instantiate the service. During instantiation of resource instances the applicable resource specifications are used. The resource instances describe what has been instantiated, the description includes which service or resource instance it supports and which resource instances it uses. Instantiation of a service is part of Automatic Product Offerings (APO), which is described in the next section, and may imply the instantiation of more resources.

First Example Use Case—Deploy Service Specification

FIG. 3 is a message flow diagram illustrating a process 300 for deploying a service specification according to some embodiments. In the example shown, process 300 beings with step 302, wherein COM agent 208 receives a Deploy Service Specification (DSS) message transmitted by a management system 389 (e.g., an Operations Support System). As used herein the term "transmits" covers not only sending a message via a network but also covers sending the message

using interprocess communication in the case of, for example, the sender (e.g., OSS or a COMPA agent) and the receiver (e.g., a COMPA agent) running on the same processing unit, as well as sending the message using a procedure call in the case of, for example, the sender and receiver being different modules of a single process. The DSS message includes a service specification that includes a service descriptor for a service. In this example, the service descriptor includes a set of two or more resource specification identifiers including a first and a second resource specification identifier (in other example the set of resource specification identifiers may consist of a single resource specification identifier). Each resource specification identifier included in the set of resource specification identifiers identifies a particular resource specification. In this example, the first resource specification identifier identifies a first resource specification that is maintained by a first RDCF **202**, and the second resource specification identifier identifies a second resource specification that is maintained by a second RDCF **392**.

The service descriptor may also include information describing the relationships, if any, between the identified resource specifications. For example, the first resource specification identifier may identify a specification for a first type of network node (e.g., Serving Gateway (SGW)) and the second resource specification identifier may identify a specification for a second type of network node (e.g., a Mobility Management Entity (MME)). In such a scenario, the service descriptor may include information indicating that SGW must be allocated in IP address and the MME must be configured with configuration information that identifies the IP address assigned to the SGW so that when the MME and SGW are instantiated the MME will be able to communicate with the SGW over an IP network.

The COM agent **208** is configured such that, in response to receiving the DSS message, COM agent **208** determines, for each resource specification identifier included in the set, whether the resource specification identified by the resource specification identifier is maintained by at least one RDCF agent. Accordingly in step **304**, COM agent **208** transmits to RDCF agent **202** a first Resource Specification Discovery (RSD) message containing the first resource specification identifier, and in step **306** COM agent **208** transmits to RDCF agent **392** a second RSD message containing the second resource specification identifier. Assuming the identified resource specifications have been previously registered with RDCF agents **202**, **392**, respectively, then the RDCF agents **202**, **392** will respond to the respective RSD with a respective positive acknowledgement (ACK) (e.g., a message comprising a pointer to the identified resource specification or comprising the resource specification itself).

COM agent **208** is further configured that, once COM agent **208** determines that each resource specification identifier included in the set identifies a resource specification that is maintained by at least one RDCF agent, COM agent **208** registers the service specification included in the DSS received from OSS **389**. That is, in step **308**, COM agent **208** transmits to RDCF **202** a Service Specification Registration (SSR) message comprising the service specification obtained from OSS **208**.

Second Example Use Case—Instantiate a Resource

FIG. **4** is a message flow diagram illustrating a process **400** for instantiating a resource. In the example shown, process **400** begins with step **402**, wherein COM agent **208** receives an Instantiate Resource (IR) message transmitted

by OSS **389**. The IR message includes a resource specification identifier that identifies a particular resource specification. In step **404**, in response to receiving the IR message, COM agent **208** transmits to RDCF **202** a Resource Specification Discover (RSD) message that comprises the resource specification identifier included in the IR message. Assuming the identified resource specification has been previously registered with RDCF agent **202**, then the RDCF agent **202** will respond to the RSD message by transmitting to COM agent **208** a message comprising a pointer to the identified resource specification or comprising the resource specification itself and COM agent will perform step **408** (and optionally **406**).

After receiving the message, COM agent **208** obtains the resource specification (extracts it from the message or uses the pointer to download it) and then parses the specification to determine information about the resource specified by the resource specification. For example, the specification may indicate that the resource should be implemented as a tenant of a multi-tenant software application. Assuming that the specification indicates that the resource should be implemented as a tenant of a multi-tenant software application, COM agent **208**, in step **406**, sends to an RDCF agent (in this case RDCF agent **392**) a Resource Instance Discovery (RID) message to determine whether an instance of the multi-tenant software application is operational.

In step **408**, COM agent deploys the resource so that the resource will be operational. For example, in the case the resource is a tenant of a multi-tenant application, then in step **408** COM agent communicates with a controller of the multi-tenant application to instantiate a new tenant corresponding to the resource. This may include COM agent **208** transmitting one or more specific configuration files corresponding to the resource. As another example, in the case that the resource is a stand-alone application, then in step **408** COM agent **208** transmits to a platform for executing the resource information contained in the Resource SW information element of the resource specification corresponding to the resource (e.g., a binary executable file and/or configuration files).

After deploying a resource, COM agent **208** may transmit to RDCF **392** a Resource Instance Registration (RIR) message or a Resource Instance Update (RIU) message (step **410**). RIR/RIU message may contain information about the deployed resource. This information about the deployed resource may contain, among other things, a service identifier identifying a service that the resource is supporting. As described above, RDCF **392**, in response to an RIR message creates a resource instance registration records that includes information included in the RIR, including the service identifier. Similarly, RDCF **392**, in response to an RIU message, updates the resource instance registration record to include information included in the RIU, including the service identifier. In this way, if a resource supports one or more services, the resource instance registration record for the resource will identify each of the one or more services. This information linking a resource to each service that the resource supports can be used by an analytics agent and/or a policy agent.

For example, an analytics agent (e.g., agent **202**) may receive from an OSS a command to monitor a particular resource. In response, the analytics agent may send to the RDCF agent that maintains the resource instance registration record for the particular resource a request to provide the analytics agent with the information stored in the registration record (or a sub-set of the information, such as the list of services that the resource supports). By having knowl-

edge of the services that the particular resource supports, the analytics agent can provide useful service information to a policy agent. For instance, if the analytics agent determines that the particular resource has become, or is on the threshold of becoming, overloaded, then the analytics agent can use the information obtained from the RDCF agent to determine the services that may be impacted by this event (i.e., the services that the particular resource supports) and then inform a policy agent not only that the particular resource is having a problem, but also can inform the policy agent that one or more identified services (i.e., the services supported by the resource) may be at risk of a performance degradation.

Similarly, a policy agent that receives from an analytics agent (or other entity) a report indicating that a particular resource is having a problem (e.g., an overload problem), the policy agent itself may send to the RDCF agent that maintains the resource instance registration record for the particular resource a request to provide the policy agent with the information stored in the registration record (or a sub-set of the information, such as the list of services that the resource supports). By having knowledge of the services that the particular resource supports, the policy agent can take an appropriate action for each service, such as, for each impacted service, instruct a COM agent to instantiate an appropriate resource for the service.

B. Automated Product Offering (APO):

APO is about automating the procedures required to instantiate a service into the network for a specific offering for specific (set of) users (this ranges from a service for an enterprise or services for a end-users). APO includes the instantiation of a service and instantiation/allocation of resources required for this service. The instantiated resources and services are registered in the resource and service inventory, respectively.

Third Example Use Case—Instantiate a Service

FIG. 5 is a message flow diagram illustrating a process 500 for instantiating a service. In the example shown, process 500 begins with step 502, wherein COM agent 208 receives an Instantiate Service (IS) message transmitted by OSS 389. The IS message comprises a service specification identifier for identifying a service specification corresponding to the service. In step 504, COM agent 208 transmits to RDCF agent 202 a Service Specification Discovery (SSD) message comprising the service specification identifier that was included in the IS message. In step 505, COM agent 208 receives from RDCF 202 the requested service specification (SS). As discussed above, the service specification comprises a set of one or more resource specification identifiers.

As a result of receiving the service specification, COM agent 208 determines, for each resource specification identifier, whether the resource corresponding to the resource specification identifier has been instantiated (i.e., is operational for the service). This is accomplished by COM agent 208 sending to one or more RDCF agents one or more RID messages. Thus, for example, in step 506, COM agent 208 transmits to an RDCF (in this example it is RDCF 392) a Resource Instance Discovery (RID) message to determine whether the corresponding resource has been instantiated. For any such resource that has not been instantiated, COM agent 208 instantiates the resource (step 508) (e.g., COM agent may perform steps 404-408).

After ensuring that all of the required resources have been instantiated (e.g., after determining that every resource identified by the one or more resource specification identifiers

included in the service specification has been instantiated), COM agent 208 registers the service instance by transmitting to RDCF 208 a Service Instance Registration (SIR) message (step 510).

C. Automated Management (AM)

AM (sometimes referred to as autonomic networks) is about automating the operational support of the network. The aim is to have a policy based control for managing the deployed and instantiated/assigned resources.

Fourth Example Use Case—Policy and Analytics Based Automatic Mgmt

FIG. 6 is a message flow diagram illustrating a process 600 for automatic management of a network. In the example shown, process 600 begins with step 602, wherein policy agent 206 transmits to analytics agent 204 a request for at least one insight (i.e., a report). The request may be a historical insight request message or a real-time insight request message. In step 604, analytics agent 204 receives data from one or more data sources (e.g., one or more resources). In some embodiments, this data includes performance information such as: number of dropped packet; memory utilization; processor utilization; number of simultaneous users; etc. In other embodiments, the data received from a resource includes information pertaining to a possible security threat. Other examples of collected data include: alarms, events from networks such as PDP context establishments, call establishments, call data records, mobility management events (e.g. location update), handover event reporting, etc.

In step 606, analytics agent 204 process the data from the data sources to generate an insight 607 based on the data received from the one or more sources and transmits the insight to policy agent 206, which receives the insight. In some embodiments, the step of transmitting the insight includes one of: transmitting an historical insight delivery message comprising the insight and transmitting a real-time insight delivery message comprising the insight.

In step 608, as a result of receiving the insight (which may include network performance information and/or security information), policy agent 206 determines whether an action is needed based on information included in the insight and a policy. For example, in step 608, policy agent 206 may execute a rule contained in a policy and determine, based on the rule and information in one or more received insights, whether a certain condition has been satisfied (e.g., whether a certain processor utilization has stayed above a certain threshold for at least a certain amount of time). As a result of determining that a network management action should be undertaken, policy agent 206, in step 610, transmits to COM agent 208 an action request 612 (e.g., a “Request Action” message or an “Instantiate Resource” message, defined above) identifying at least one specific action. In step 612, COM agent 208 performs the requested action(s).

Sixth Example Use Case—Cross-Domain Management

This use case is used to illustrate that an analytics agent 704 (see FIG. 7) in one RD may receive insights from other analytics agents (i.e., agents 702 and 204) each of which belongs to an RD different than the RD to which agent 704 belongs, and a policy agent 706 can use insights generated by agent 704 to determine whether an action should be undertaken. Additionally, agents 702 and 204 may belong to different RDs.

Referring now to FIG. 7, which illustrates an example process 700, in step 701, policy agent 706 transmits to agent 704 a request for at least one insight. In step 702, agent 704 transmits to agent 204 a request for at least one insight (the request may be a historical insight request message or a real-time insight request message). In step 704, agent 704 transmits to agent 702 a request for at least one insight (the request may be a historical insight request message or a real-time insight request message).

In step 706, analytics agent 204 generates an insight based on data received from one or more resources and transmits the insight to analytics agent 704, which receives the insight. In step 708, analytics agent 702 generates an insight based on data received from one or more resources and transmits the insight to analytics agent 704, which receives the insight. In step 710, analytics agent 704 generates an insight based on the insights received in steps 706 and 708 and transmits the generated insight to policy agent 706.

In step 712, as a result of receiving the insight transmitted by agent 704, policy agent 706 determines whether an action is needed based on information in the insight and a policy. As a result of determining that an action should be undertaken, policy agent 706 transmits to COM agent 708 an action request identifying at least one specific action.

In some embodiments, an analytics agent (e.g., agent 204) is configured to transmit to a policy agent (e.g., agent 206) a real-time insight delivery message in response to detecting that a certain condition or event has been detected. For example, in response to detecting that a performance parameter (e.g., a load on a service) has met or exceeded a threshold or in response to detecting some other event or condition.

In some embodiments, policy agent 206 is configured such that, after receiving the real-time insight, the policy agent 206 determines whether more actions should be undertaken (e.g., policy agent execute a policy statement). For example, in response to receiving a real-time insight indicating that a load on a service has met or exceeded a threshold, policy agent 206 may be configured by a policy statement to determine whether resources should be added to the service and may further be configured such that, in response to determining that more resources should be added to the service, the policy agent 206 transmits to a COM agent (e.g., COM agent 208) a message requesting that the COM agent add more resources to the service (e.g., agent 206 transmits to agent 208 an Instantiate Resource message). As another example, in response to receiving a real-time insight indicating that a subscriber notification is required or that a subscriber should be blocked, policy agent 206 may be configured to send a message to a COM agent to cause the COM agent to provide a certain notification to the subscriber or block the subscriber.

FIG. 8 is a flow chart illustrating a method 800 in COMPA system 200 comprising, a first analytics agent (e.g., analytics agent 204), a first policy agent (e.g., policy agent 206), and a first COM agent (e.g., COM agent 208). The first analytics agent is configured to collect data from various data sources, process the collected data to generate insights, and provide requested insights to a consuming agent (e.g., a policy agent 206) as a result of receiving from the consuming agent a report request identifying a requested insight type. Process 800 may begin in step 802, where the first policy agent requests the first analytics agent to send to the first policy agent one or more insights. In step 804, the first policy agent, in response to receiving a set of one or more insights from the first analytics agent, uses a policy statement and the set of one or more insights to determine whether a first action

should be taken. In step 806, as a result of determining the first action should be taken, the first policy agent transmits to the first COM agent a first action request message for identifying the first action, the first COM agent being configured such that, in response to receiving the first action request message, the first COM agent performs the requested first action.

In some embodiments, method 800 includes additional steps (see e.g., FIG. 7). For example, method 800 may further include: a second analytics agent (e.g., analytics agent 702) collecting data from various data sources, processing the collected, and providing requested insights; and a third analytics agent (e.g., analytics agent 704) requesting the first analytics agent to send to the third analytics agent one or more insights generated by the first analytics agent and requesting the second analytics agent to send to the third analytics agent one or more insights generated by the second analytics agent. The method may further include the third analytics agent generating at least one insight based at least in part on one or more insights transmitted to the third analytics agent from the first analytics agent and one or more insights transmitted to the third analytics agent from the second analytics agent.

In some embodiments, the method also includes a second policy agent (e.g., policy agent 706) requesting the third analytics agent to send to the second policy agent one or more insights generated by the third analytics agent based at least in part on one or more insights transmitted to the third analytics agent from the first analytics agent and one or more insights transmitted to the third analytics agent from the second analytics agent. The second policy agent, in response to receiving a set of one or more insights from the third analytics agent, may use a policy and the set of one or more insights received from the third analytics agent to determine whether a second action should be taken, and, as a result of determining the second action should be taken, transmits to a second COM agent (e.g. COM agent 708) a second action request message for identifying the second action, and the second COM agent is configured such that, in response to receiving the second action request message, the second COM agent performs the requested second action.

FIG. 9 is a flow chart illustrating a process 900 for service onboarding, according to some embodiments. Process 900 may begin with step 902, in which a first COM agent (e.g., COM agent 208) receives from a support system a first request to deploy a service specification. The first request to deploy the service specification includes a service descriptor for the service, the service descriptor includes a set of one or more resource specification identifiers including a first resource specification identifier. Each resource specification identifier included in the set of resource specification identifiers identifies a particular resource specification. The first resource specification identifier identifies a first resource specification that is maintained by a first RDCF agent (e.g., RDCF agent 202). In step 904, the first COM agent, in response to receiving the first request to deploy the service specification, selects a resource specification identifier (RSI) from the set of RSIs. In step 906, the first COM agent, determines whether the resource specification identified by the selected RSI is maintained by at least one RDCF agent. If not, the process may proceed to step 910, where the first COM agent transmits an error message to the support system, otherwise the process proceeds to step 908 in which the first COM agent determines whether it has selected each one of the RSIs included in the set of RSI. If one or more RSIs in the set have not yet been selected, the process goes back to step 904.

FIG. 10 is a flow chart illustrating a process 1000 for automatic product offering. Process 1000 may begin with step 1002 in which the first COM agent receives from a support system a first request to instantiate a service. The first request to instantiate the service includes a service specification identifier identifying a service specification that includes a list of required resources. In step 1004, the first COM agent, in response to receiving the first request to instantiate the service, transmits to the RDCF agent a service specification discovery request that includes the service specification identifier. The RDCF agent is configured such that, in response to receiving the service specification discovery request comprising the service specification identifier, the RDCF agent uses the service specification identifier to retrieve the service specification identified by the service specification identifier and transmit the retrieved service specification to the first COM agent. In step 1006, the first COM agent receives from the RDCF agent the retrieved service specification. In step 1008, the first COM agent, in response to receiving the service specification from the RDCF agent, determines, for at least one of the required resources identified in the list of required resources included in the service specification, whether the at least one required resource has been instantiated. In step 1010 (optional), the COM agent instantiates one or more of the required resources that are not already instantiated (e.g., the COM agents performs steps 404-408).

IV. COMPA Adapter Agents

A COMPA system may employ one or more COMPA adapter agents. In one aspect, a COMPA adapter agent (“adapter”) provides COMPA interfaces and COMPA framework procedures as an add-on to implementations of A, P, COM, RDCF, and SAC functionality. The adapters can be used to adapt both existing and new non-COMPA implementations (i.e., “legacy” implementations) to a COMPA architecture (framework), and to build new COMPA adapted implementations.

FIG. 11 illustrates an example adapter apparatus 1100 (e.g., a gateway) includes a an adapter 1104 for providing services to a consumer 1101 of COMPA services (this consumer could be a COMPA agent) and for communicating with at least one legacy agent 1108. Adapter 1104 may also be configured to communicate with one or more COMPA agents. In this example, adapter 1104 may function as proxy that translates a COMPA message 1110 received at the adapter apparatus 1100 from the consumer 1101 into a legacy message 1111 and that sends the legacy message 1111 to the legacy agent 1108. Additionally, the adapter 1104 functions to receive a legacy response 1112 from the legacy agent 1108 and translate the response to a COMPA response message 1113 and then provides the translated response 1113 to the consumer 1101. In this way, adapter apparatus 1100 enables consumer 1101 to invoke an operation by the legacy agent 1108 using a COMPA message that legacy agent 1108 is not operable to successfully process. FIG. 12 illustrates an example apparatus 1200 that includes both adapter 1104 and a COMPA agent 1213 (e.g., Analytics, Proxy, COM, RDCF).

FIG. 13 illustrates adapter 1104 according to some embodiments. As shown in FIG. 13, adapter 1104 may include three layers, COMPA Interface Provider (C-IP) 1301, COMPA Configuration Framework Manager (C-CFM) 1302, and COMPA Service Provider Interface (C-SPP) 1303, with a COMPA Framework Application Programming Interface (C-FRAPI) 1311 between C-IP and C-CFM and a COMPA Service Provider Interface (C-SPI) 1312 between C-CFM and C-SPP. C-IP implements

COMPA interfaces and C-SPP implements, among other things, legacy interfaces and/or implementations of A, P, COM and RDCF.

A. COMPA Interface Providers (C-IP)

A C-IP implements a COMPA interface—e.g. an Analytics, Policy COM or RDCF interface. That is, a C-IP includes a COMPA plug-in (CPI) 1322 that is configured to understand and act on a set of COMPA messages. For example, a C-IP that implements an Analytics interface is typically configured with a CPI that is configured to understand and act on the COMPA Analytics messages described in Tables 1-4 above. In some embodiments, a C-IP includes a generic CPI that is common for all RDs and a specialized CPI (a.k.a., Specialized Domain Package (SDP)) that is specific for the RD to which the adapter 1104 belongs. SDPs carry information (parameters) that are only relevant for a particular RD, e.g. parameters applicable only for the packet network or transport network domains. When an SDP is loaded into C-IP 1301 of adapter 1104, the SDP specializes the adapter for the domain in which it is to be applied.

B. COMPA Configurable Framework Manager (C-CFM)

C-CFM contains logic for mapping COMPA interfaces onto Service Provider Plug-ins (SPPs) in C-SPP. It is configurable to handle the protocol extensions the Specialized Domain Packages introduce and includes functionality for: (i) loading a Specialized Domain Package (SDP) and configuring the C-IP to support the SDP; (ii) loading and binding to C-SPP Plug-ins; and (iii) automatic registration of service capabilities with COMPA RDCF functionality, to enable service capability discovery. C-CFM has the overall responsibility and orchestrates the activities performed by a COMPA Adapter, i.e. ties together the actions performed by C-IP and C-SPP.

C. COMPA Service Provider Plug-Ins (C-SPP)

The C-SPP layer includes one or more Service Provider Plug-ins (SPPs) as well as one or more CPIs. Each SPP is used to interact with non-COMPA implementations of A, P, COM and RDCF functionality, both existing and new implementations. An SPP is a software package, which may implement an API or an external protocol.

For example, as shown in FIG. 14, C-SPP layer 1303 of COMPA Adapter 1104 may include one or more of SPPs 1402-1406 and a CPI 1410. In the example shown, the C-SPP 1303 includes the following SPPs: an SPP 1402 (SPP1) for providing an interface to a legacy COM agent; an SPP 1404 (SPP2) for providing an interface to a legacy, proprietary Policy function; and an SPP 1406 (SPP3) for providing an interface to a legacy Analytics agent. The C-SPP 1303, in this example, also includes a CPI 1410 for transmitting COMPA Analytics messages to (and receiving and processing COMPA messages from) a COMPA Analytics agent 1450.

FIG. 15 illustrates an example use case. In this use case adapter 1104 is an RDCF adapter that is able to obtain capability information from both legacy agent 1108 (which in this example is a legacy service catalog) and a COMPA RDCF agent 1591. More specifically, the C-IP layer 1301 includes CPI 1512 for receiving and processing COMPA RDCF messages (e.g., the C_Service Capability Discovery message); the C-SPP layer 1303 includes an SPP 1522 for obtaining capability information from legacy service catalog 1108 and includes a CPI 1524 for obtaining capability information from COMPA RDCF agent 1591; and the C-CFM layer 1302 includes a SW 1526 for, among other things, causing C-SPP to send messages to legacy service catalog 1108 and COMPA RDCF agent 1591 in response to C-IP receiving a C_Service Capability Discovery message.

Further functionality performed by adapter **1104** is illustrated in the message flow diagram shown in FIG. **16**.

FIG. **16** is a message flow diagram illustrating a process **1600** according to an example embodiment. As shown in FIG. **16**, the process **1600** may begin with a consumer (e.g., a COMPA Policy agent) transmitting to adapter **1104** a C_Service Capability Discovery message requesting a list of all types of analytics that are available (step **1602**). This message is received by CPI **1512**, which, in this embodiment, extracts parameters from the message and provides the extracted parameters to SW **1526** (step **1604**). The extracted parameters inform SW **1526** that a consumer is requesting analytics capability information.

In step **1606**, SW **1526**, based on stored configuration information, determines that analytics capability request messages should be sent to legacy service catalog **1108** and RDCF **1591**. For example, in step **1606**, SW **1526** searches an internal database to discover all of the available sources of analytics capability information and, for each discovered information source, how the discovered information source should be accessed. In this example, SW **1526** discovers that the legacy service catalog **1108** and COMPA RDCF agent **1591** are the available information sources and that the sources are accessed via SPP **1522** and CPI **1524**, respectively.

In step **1608**, SW **1526** provides to SPP **1522** parameters for enabling SPP **1522** to send an analytics capability request message to legacy service catalog **1108**. These parameters may include the address of legacy service catalog **1108** as well as one or more parameters that were contained in the C_Service Capability Discovery message and/or derived from parameters contained in the C_Service Capability Discovery message.

In step **1610**, SPP **1522** receives the parameters, generates an analytics capability request message, and transmits the analytics capability request message to legacy service catalog **1108**.

In step **1612**, SPP **1522** receives from legacy service catalog **1108** a result message comprising analytics capability information (e.g., "Packet Core Analytics 3G service" and "Packet Core Analytics 4G service"). In step **1614**, SPP **1522** provides the received analytics capability information to SW **1526**.

In step **1616**, SW **1526** provides to CPI **1524** parameters for enabling CPI **1524** to send a C_Service Capability Discovery message to RDCF **1591**. These parameters may include the address of RDCF **1591** as well as one or more parameters that were contained in the C_Service Capability Discovery message and/or derived from parameters contained in the C_Service Capability Discovery message.

In step **1618**, CPI **1524** receives the parameters, generates the C_Service Capability Discovery message, and transmits the message to RDCF **1591**.

In step **1620**, CPI **1524** receives from RDCF **1591** a C_Service Capability Discovery Response message comprising analytics capability information (e.g., "Analytics for optical transport networks"). In step **1622**, CPI **1524** provides the received analytics capability information to SW **1526**.

In step **1624**, SW **1526** provides to CPI **1512** the analytics capability information received from legacy service catalog **1108** via SPP **1522** and the analytics capability information received from RDCF **1591** via CPI **1524**.

In step **1626**, CPI **1512** generates a response to the C_Service Capability Discovery transmitted by the consumer and transmits the response to the consumer. The response includes the analytics capability information

received from legacy service catalog **1108** and the analytics capability information received from RDCF **1591**. In this way, the consumer is able to use a single COMPA discover message to obtain information maintained by a legacy agent as well as information maintained by a COMPA agent.

FIG. **17** illustrates another example adapter use case. In the example shown, a system **1700** includes two adapters (adapter **1104a** and adapter **1104b**), a policy agent **1706**, RDCF agent **1591**, a first agent **1108a** (which in this case is a legacy transport analytics agent) and a second legacy agent **1108b** (which in this case is a transport management agent) for managing transport functions **1714**. Adapter **1104a** functions a COMPA Analytics proxy and adapter **1104b** functions as a COMPA COM proxy.

FIG. **18** is a message flow diagram illustrating a process **1800** performed, at least in part, by system **1700**. Process **1800** begins with an administrative entity (e.g., a COMPA manager **1882**) providing an SPP **1884** to C-CFM **1302a** of adapter **1104a** (step **1801**). SPP **1884** is a plug-in designed to enable adapter **1104a** to request and obtain analytics from legacy transport analytics agent **1108a**. In step **1802**, C-CFM **1302a** adds SPP **1884** to C-SPP layer **1302a** of adapter **1104a**, initializes SPP **1884**, and causes SPP **1884** to transmit a message to transport analytics agent **1108a** to confirm that SPP **1884** is able to communicate with transport analytics agent **1108a**. In step **1803**, SPP **1884** transmits the message to transport analytics agent **1108a**. In step **1804**, SPP **1884** receives from transport analytics agent **1108a** an acknowledgement (ACK) to the message, which SPP **1884** provides to C-CFM in step **1805**. In step **1806**, C-CFM transmits an ACK to manager **1882** to inform manager **1882** that SPP **1884** has been successfully loaded.

In step **1807**, manager **1882** provides an SW **1886** (e.g., an SDP) to C-IP **1301a** of adapter **1104a**. SW **1886** is a software package that is configured to enable C-IP **1301a** to receive a message (e.g., a transport analytics request) transmitted by a consumer (e.g., Policy agent **1706**) and process the message to cause the adapter **1104a** to request and obtain analytics from legacy transport analytics agent **1108a**. Upon receiving SW **1886**, C-IP **1301a** informs a service catalog of its new capability to process transport analytics requests. For example, in step **1808**, C-IP **1301a** transmits to RDCF **1591** a C_Service Capability Registration message comprising information indicating that the adapter **1104a** is now capable of providing transport analytics (e.g., reports regarding a transport network). In step **1809**, C-IP **1301a** receives an ACK from RDCF **1591**, which then causes C-IP **1301a** to transmit an ACK to manager **1882** indicating that new capability has been registered.

A process similar to process **1800** may be performed for adapter **1104b**. For example, manager **1882** may be configured to provide to adapter **1104b** an SPP for enabling adapter **1104b** to request transport management agent **1108b** to perform one or more management functions and an SDP configured to enable adapter **1104b** to receive a message (e.g., a COM message defined in Table 7) transmitted by a consumer (e.g., Policy agent **1706**) and to employ the SPP to forward to transport management agent **1108b** one or more parameters from the COM message (or legacy parameters derived from the parameters included in the COM message).

FIG. **19** is a message flow diagram illustrating a process **1900** performed, at least in part, by system **1700**. Process **1900** begins with Policy agent **1706** transmitting to RDCF agent **1591** a C_Service Capability Discovery message requesting information on which COMPA analytics agent or adapter is capable of providing transport analytics (step

1901). In step 1902, RDCF 1591 responds by transmitting to Policy 1706 a C_Service Capability Discovery Response message comprising information indicating that adapter 1104a has the capability of providing transport analytics and an address (e.g., URN) for accessing adapter 1104a. After receiving the response, Policy 1706 uses the address obtained from RDCF 1591 to transmit to adapter 1104a a real-time insight request message with the Requested Insight Type IE of the message comprising information identifying that the requestor is requesting transport analytics (step 1903). This message is received by C-IP 1301a, which extracts relevant parameters from the message and provides the extracted parameters to C-CFM 1302a using a message indicating that the requestor is requesting real-time analytics delivery (step 1904). In step 1905, derives one or more legacy parameters based on the information provided by C-IP 1301a in step 1904. For example, C-CFM 1302a may maintain a parameter map for mapping COMPA parameters to the legacy parameters.

In step 1906, C-CFM 1302a provides to C-SPP 1303a a message comprising the legacy parameters (if any) and information indicating that C-SPP 1303a should transmit to transport analytics 1108a an insight delivery request comprising the legacy parameters. Depending on the capabilities of transport analytics 1108a, C-SPP may either: (i) send to transport analytics 1108a an analytics subscription request specifying one or more conditions under which transport analytics 1108a should provide an analytics message (e.g., a status report) to the requestor (step 1907a) or (ii) start polling transport analytics 1108a for analytics (i.e., periodically transmit to transport analytics 1108a an analytics request) (step 1907b). In step 1908, transport analytics 1108a, in response to the subscription request sent in step 1907a or the analytics request sent in step 1907b, transmits to adapter 1104a the requested insight. For example, if transport analytics 1108a has the capability to handle an analytics subscription request, then in response to receiving the analytics subscription request sent in step 1907a, transport analytics 1108a will configure itself to transmit to adapter 1104a an insight whenever one of the specified conditions are met.

The insight transmitted by transport analytics 1108a is received by C-SPP 1303a, which extracts information (e.g., parameters) from the insight and provides the extracted information to C-CFM 1302a (step 1909). In step 1910, C-CFM 1302a uses stored configuration information to process the information, if necessary (e.g., map legacy parameters to COMPA parameters); and then C-CFM 1302a sends (step 1911) a message to C-IP 1301a causing C-IP 1301a to transmit to Policy 1706 an insight (step 1912) comprising the information extracted by C-SPP 1303a and/or the processed information. Policy 1706 may then decide whether it needs to act on the insight by, for example, sending a COMPA COM message to adapter 1104b.

If Policy 1706, as a result of receiving the insight from adapter 1104a, sends to adapter 1104b a COMPA COM message for causing a certain management action to occur, then adapter 1104b, in response, may be configured to send to transport management agent 1108b a management request message for causing the transport management agent 1108b to perform the management action (e.g., deploy a new transport resource). For example, the COMPA COM message may be received by the C-IP of adapter 1104b and it may extract parameters from the message and provide the parameters to the C-CFM of adapter 1104b, which maps the parameters to legacy parameters and provides the legacy parameters to C-SP of adapter 1104b, which will then

generate a management request message comprising the legacy parameters and send the management request message to transport management agent 1108b.

FIG. 20 is a flow chart illustrating a process 2000, according to some embodiments, for enabling a consumer (e.g., consumer 1101) to invoke an operation by legacy agent 1108 using a message that legacy agent 1108 is not operable to successfully process. Process 2000 begins with step 2002, in which adapter 1104 receives a software package (e.g., SW 1886) for use in processing the message. In step 2004, the adapter, as a result of loading the software package, transmits to RDCF agent 1591 a capability registration message comprising information indicating that the adapter is configured to process the message.

FIG. 21 is a flow chart illustrating a process 2100, according to some embodiments, for enabling a consumer (e.g., consumer 1101) to invoke an operation by legacy agent 1108 using a message that legacy agent 1108 is not operable to successfully process. Process 2100 begins with step 2102, in which adapter 1104 receives a software package (e.g., SPP 1522 or 1884) for use in communicating with the legacy agent using a legacy interface implemented by the legacy agent. In step 2104, the adapter, after loading the software package, transmits a message to the legacy agent to confirm that the adapter apparatus is operable to communicate with the legacy agent. In step 2106, the adapter receives from the legacy agent a response to the message sent in step 2104. After the adapter confirms that the adapter is operable to communicate with the legacy agent (i.e., after receiving the response), the adapter performs steps 2002 and 2004 of process 2000.

In some embodiments, the message is a request for an insight delivery, and the adapter is further configured such that, upon receiving the message, the adapter maps a parameter included in the message to a legacy parameter, generates a legacy message comprising the legacy parameter, and transmits the legacy message to the legacy agent. In other embodiments, the message is a request for a policy decision, and the legacy agent is a legacy policy agent. In yet other embodiments, the message is a request for a network management operation, and the legacy agent is a legacy network management agent.

FIG. 22 is a flow chart illustrating a process 2200, according to some embodiments. In some embodiments, process 2200 is performed by adapter 1104 after adapter 1104 performs process 2000 or process 2100. Process 2200 begins with step 2202, in which adapter 1104 receives from a consumer a capability discovery message indicating that the consumer is requesting certain capability information. As a result of receiving the message, the adapter: extracts a parameter from the capability discovery message (step 2204); uses the extracted parameter to determine an identifier (e.g., IP address or name that can be resolved to an address) for a legacy agent that maintains the requested capability information (step 2206); and uses the determined identifier to transmit to the legacy agent a legacy message requesting the certain capability information (step 2208). In step 2210, the adapter receives from the legacy agent a legacy response message comprising capability information selected by the legacy agent in response to the legacy message transmitted by the adapter to the legacy agent. In step 2212, the adapter forwards the capability discovery message to the RDCF 1591, which is configured to respond to the message by transmitting to the adapter retrieved capability information. In step 2214, the adapter receives from RDCF a discovery response comprising capability information obtained by the RDCF 1591. In step 2216, the

adapter transmits to the consumer a capability discovery response message, wherein the capability discovery response message comprises the capability information included in the legacy response message and the capability information included in the discovery response transmitted by RDCF **1591**.

In some embodiments, in response to a certain trigger, the adapter **1104** transmits to the RDCF **1591** an update capability message comprising updated capability information for the adapter. In yet some other embodiments, in response to a certain trigger, the adapter **1104** transmits to the RDCF **1591** a delete capability message comprising an identifier identifying a capability that the RDCF **1591** should delete from a capability record for the adapter **1104**.

FIG. **23** is a block diagram of a computer system **2300** that can be used to implement one or more of the above described agents. That is, in some embodiments, for each of the above described agents, the network **100** has a separate computer system **2300** for implementing the agent, but in other embodiments, one or more agents may be implemented using only a single computer system **2300**. For example, adapter apparatus **1100** may include computer system **2300**. As described below, computer system **2300** may consist of a single computer apparatus or set of computer apparatuses (i.e., computer system **2300** may be a cloud computing system).

As shown in FIG. **23**, computer system **2300** includes at least one computer apparatus (CA) **2302**, which may include one or more processors **2355** (e.g., one or more general purpose microprocessors and/or one or more data processing circuits, such as an application specific integrated circuit (ASIC), field-programmable gate arrays (FPGAs), logic circuits, and the like). In some embodiments, computer system **2302** includes a plurality of CAs **2302**, which may or may not be co-located. Thus, the above described adapters and agents may be implemented in a cloud computing environment. In some embodiments, each agent and each adapter may correspond to a virtual machine hosted by computer system **2300**. Computer system **2300** further includes: a network interface **2305** for use in transmitting and receiving data via a communications link; and a data storage system **2308**, which may include one or more non-volatile storage devices and/or one or more volatile storage devices (e.g., random access memory (RAM)). In embodiments where computer apparatus **2302** includes a microprocessor, a computer program product (CPP) **2341** may be provided. CPP **2341** includes a computer readable medium (CRM) **2342** storing a computer program (CP) **2343** comprising computer readable instructions (CRI) **2344**. CRM **2342** may be a non-transitory computer readable medium, such as, but not limited to, magnetic media (e.g., a hard disk), optical media (e.g., a DVD), memory devices (e.g., random access memory), and the like, but not a signal. In some embodiments, the CRI of computer program **2343** is configured such that when executed by data processing system **2302**, the CRI causes the computer apparatus **2302** to perform steps described above. In other embodiments, apparatus **2302** may be configured to perform steps described herein without the need for code. That is, for example, apparatus **2302** may consist merely of one or more ASICs. Hence, the features of the embodiments described herein may be implemented in hardware and/or software.

While various embodiments of the present disclosure are described herein, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present disclosure should not be limited by any of the above-described exemplary embodi-

ments. Moreover, any combination of the above-described elements in all possible variations thereof is encompassed by the disclosure unless otherwise indicated herein or otherwise clearly contradicted by context.

Additionally, while the processes described above and illustrated in the drawings are shown as a sequence of steps, this was done solely for the sake of illustration. Accordingly, it is contemplated that some steps may be added, some steps may be omitted, the order of the steps may be re-arranged, and some steps may be performed in parallel.

The invention claimed is:

1. A method for enabling a first consumer to invoke an operation by a legacy agent using a message that the legacy agent is not operable to successfully process the message, comprising:

an adapter receiving a first software package for use in processing the message; and

the adapter, as a result of loading the first software package, transmitting to a Responsibility Domain Common Functions, RDCF, agent a capability registration message comprising information indicating that the adapter is configured to process the message,

the adapter receiving from a second consumer a capability discovery message indicating that the second consumer is requesting certain capability information;

after receiving the capability discovery message, the adapter: extracting a parameter from the capability discovery message, using the extracted parameter to determine an identifier for a second legacy agent that maintains the requested capability information, and using the determined identifier to transmit to the second legacy agent a second legacy message requesting said certain capability information;

the adapter receiving from the second legacy agent a legacy response message comprising capability information selected by the second legacy agent in response to the second legacy message transmitted by the adapter to the second legacy agent; and

after receiving the legacy response message, the adapter transmitting to the second consumer a capability discovery response message comprising the capability information included in the legacy response message.

2. The method of claim **1**, further comprising the adapter receiving a second software package for use in communicating with the legacy agent using a legacy interface implemented by the legacy agent; and

the adapter, after loading the second software package, transmitting a message to the legacy agent to confirm that the adapter apparatus is operable to communicate with the legacy agent.

3. The method of claim **2**, wherein the adapter transmits the capability registration message to the RDCF after the adapter confirms that the adapter is operable to communicate with the legacy agent.

4. The method of claim **1**, wherein the message is a request for an insight delivery, and

the method further comprises the adapter: mapping a parameter included in the message to a legacy parameter, generating a legacy message comprising the legacy parameter, and

transmitting the legacy message to the legacy agent.

5. The method of claim **1**, wherein the message is a request for a policy decision, and the legacy agent is a legacy policy agent.

6. The method of claim **1**, wherein the message is a request for a network management operation, and the legacy agent is a legacy network management agent.

7. The method of claim 1, wherein the method further comprises the adapter, after receiving the capability discovery message, forwarding the capability discovery message to the RDCF, which is configured to respond to the message by transmitting to the adapter retrieved capability information, and the capability discovery response message further comprises the capability information retrieved by and received from the RDCF.

8. The method of claim 1, further comprising: in response to a certain trigger, the adapter transmitting to the RDCF agent an update capability message comprising updated capability information for the adapter.

9. The method of claim 1, further comprising: in response to a certain trigger, the adapter transmit to the RDCF agent an delete capability message comprising an identifier identifying a capability that the RDCF agent should delete from a capability record for the adapter.

10. A computer program product comprising a non-transitory computer readable medium storing a computer program comprising instructions for performing the method of claim 1.

11. An adapter apparatus for enabling a first consumer to invoke an operation on a legacy agent using a message that the legacy agent is not operable to successfully process the message, comprising:

a data storage system, and

a computer apparatus coupled to the data storage system, the computer apparatus comprising one or more processors, wherein the adapter apparatus is configured such that, after an administration entity loads onto the adapter apparatus a first software package for use in processing the message, the adapter apparatus:

transmits to an Responsibility Domain Common Functions, RDCF, agent a capability registration message comprising information indicating that the adapter apparatus is configured to process the message; and provide to the administration entity a message indicating that the adapter apparatus has successfully registered with the RDCF information indicating that the adapter apparatus is configured to process the message,

wherein the adapter apparatus is further configured such that, upon receiving from a second consumer a capability discovery message indicating that the second consumer is requesting certain capability information, the adapter:

extracts a parameter from the capability discovery message;

uses the extracted parameter to determine an identifier for a second legacy agent that maintains the requested capability information; uses the determined identifier to transmit to the second legacy agent a second legacy message requesting said certain capability information; and

transmits to the second consumer a capability discovery response message after receiving from the second legacy agent a legacy response message comprising capability information selected by the second legacy agent in response to the second legacy message transmitted by the adapter apparatus, wherein the capability discovery response message comprises the capability information selected by and received from the second legacy agent.

12. The adapter apparatus of claim 11, wherein the adapter apparatus is further configured such that, after an administration entity loads onto the adapter apparatus a second software for use in processing the message, the adapter apparatus transmits a message to the legacy agent to confirm that the adapter apparatus is operable to communicate with the legacy agent.

13. The adapter apparatus of claim 12, wherein the adapter apparatus transmits the capability registration to the RDCF after the adapter apparatus confirms that the adapter apparatus is operable to communicate with the legacy agent.

14. The adapter apparatus of claim 11, wherein the message is a request for an insight delivery, and

the adapter apparatus is further configured such that, upon receiving the message, the adapter apparatus maps a parameter included in the message to a legacy parameter, generates a legacy message comprising the legacy parameter, and transmits the legacy message to the legacy agent.

15. The adapter apparatus of claim 11, wherein
i) the message is a request for a policy decision, and the legacy agent is a legacy policy agent or
ii) the message is a request for a network management operation, and the legacy agent is a legacy network management agent.

16. The adapter apparatus of claim 14, wherein the adapter apparatus is further configured such that, after receiving the capability discovery message, the adapter apparatus further forwards the capability discovery message to the RDCF, which is configured to respond to the message by transmitting to the adapter apparatus retrieved capability information, and the capability discovery response message further comprises the capability information retrieved by and received from the RDCF.

17. The adapter apparatus of claim 11, wherein the adapter apparatus is further configured such that, in response to a certain trigger, the adapter apparatus transmit to the RDCF agent an update capability message comprising updated capability information for the adapter apparatus.

18. The adapter apparatus of claim 11, wherein the adapter apparatus is further configured such that, in response to a certain trigger, the adapter apparatus transmit to the RDCF agent an delete capability message comprising an identifier identifying a capability that the RDC agent should delete from a capability record for the adapter apparatus.